DATA PROCESSING ADDENDUM

This Data Processing Addendum, including its Exhibits, ("DPA"), forms a part of the Master Services Agreement found at https://vtex.com/us-en/agreements/ unless the Contractor has entered into a superseding written Master Services Agreement with VTEX, in which case, it forms a part of such written agreement. Together, the Master Services Agreement and the Order Form - Commercial Proposal, are referred to as the "Agreement".

By signing the DPA, the Contractor enters into this DPA on behalf of itself and, to the extent that applicable Data Protection Laws require that a Controller Affiliate enters into a DPA with VTEX as well, in the name and on behalf of its Controller Affiliates (defined below).

For the purposes of this DPA only, and except where indicated otherwise, the term "Contractor" shall include the Contractor and those Controller Affiliates required by applicable Data Protection Laws to enter into a DPA with VTEX. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

In the course of providing the Services under the Agreement, VTEX may Process certain Personal Data (such terms defined below) on behalf of Contractor and where VTEX Processes such Personal Data on behalf of Contractor, the Parties agree to comply with the terms and conditions in this DPA in connection with such Personal Data.

HOW TO EXECUTE THIS DPA?

1. This DPA consists of two parts: the main body of the DPA, and its 2 appendices:

- **Appendix 1: Description of the Processing:** Appendix 1 sets out certain information regarding the conditions of Processing resulting from the Services provided by VTEX under the Agreement.
- **Appendix 2: Technical and Organizational Measures**

2. Contractor acknowledges and agrees that it was aware of the clauses set forth in this DPA when signing the Order Form - Commercial Proposal.

HOW THIS DPA APPLIES TO CONTRACTOR AND ITS AFFILIATES?

If the Contractor entity signing this DPA is the Contractor under the Agreement, this DPA is an addendum to and forms part of the Agreement. If the Contractor Affiliate is a contractual party to this DPA by effect of Section 8 below, this DPA is binding onto VTEX and this Contractor Affiliate. In such a case, references to "VTEX" in this DPA shall mean the VTEX entity that is party to the Agreement.

If the Contractor entity signing this DPA has executed an Order Form - Commercial Proposal with VTEX or its Affiliate pursuant to the Agreement, but is not itself a party to the Agreement, this DPA is an addendum to that Order Form - Commercial Proposal and applicable renewal Order Form - Commercial

Proposals, and references to “VTEX” in this DPA shall mean the VTEX entity that is party to such Order Form - Commercial Proposal.

1. DEFINITIONS

For the purposes of this DPA, any terms in capitalized letters that are not defined below or otherwise in this DPA or in the applicable Data Protection Laws, will have the meanings given to them in the Agreement.

“**Affiliate**” means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. “Control", for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

“**Authorized Users**” means any person authorized by VTEX in writing to have control over a a VTEX Platform environment and any person who is given access by Contractor to a VTEX Platform environment in accordance with the requirements set out in the Agreement.

“**Controller**” means the entity which determines the purposes and means of the Processing of Personal Data.

"**Controller Affiliate**" means any of Contractor's Affiliate(s): (a)(i) that are subject to applicable Data Protection Laws, and (ii) are permitted to use the Services pursuant to the Agreement between Contractor and VTEX, but have not signed their own Order Form - Commercial Proposal and are not a “Contractor” as defined under the Agreement, and (b) if and to the extent VTEX processes Personal Data for which such Affiliate(s) qualify as the Controller.

“**CCPA**” means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., and its implementing regulations.

“**Contractor**” means the entity that is the contracting party to the Agreement and that is signing this DPA, on behalf of itself and on behalf of any and all Contractor Affiliates, as the case may be.

“**Contractor Data**” means all data and information submitted by Authorised Users to the Services and includes message text, files, comments and links, excluded Non-VTEX Products. Contractor Data does not include any Personal Data relating to Authorised Users received for the purposes of authorising access to the Services, or the representatives of the Contractor or Contractor Affiliates in connection with execution and administration of the Agreement or this DPA, which Personal Data VTEX processes as a controller.

“**Data Protection Laws**” means all laws and regulations, including laws and binding regulations applicable to the Processing of Personal Data under the Agreement, as amended from time to time, including: (a) the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 (the “CCPA”), the Virginia Consumer Data Protection Act of 2021 (“VCDPA”), the Colorado Privacy Act of 2021 (“CPA”), the Health Insurance Portability and Accountability Act ("HIPAA"), and the GDPR, and (b) any guidance or statutory codes of practice issued or adopted by any Supervisory Authority or other applicable data protection authority or a Data Protection Boards in relation to such legislations, in any case as applicable to the Processing of Personal Data under the Agreement and other

applicable data privacy laws or regulations, including laws, regulations, or other regulatory guidance ratifying, implementing, adopting, supplementing, or replacing the CCPA, VCDPA, CPA, HIPAA or GDPR; in each case to the extent in force and as such are updated, amended, or replaced from time to time.

"**Data Subject**" means the identified or identifiable person to whom Personal Data relates, and shall include any person whose Personal Data is subject to protection under, or who has any legally exercisable rights under, any Data Protection Laws.

"**Personal Data**" means any Contractor Data that relates to an identified or identifiable natural person, to the extent that such information is protected as personal data, personal information, personally identifiable information (or words of similar meaning), under applicable Data Protection Laws.

"**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

"**Processing**" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"**Processor**" means the entity which Processes Personal Data on behalf of the Controller, including as applicable any "service provider" as that term is defined by the CCPA.

"**Sub-processor**" means any entity engaged by VTEX, including a member of the VTEX Group as a sub-processor, to Process Personal Data in connection with the Services.

"**Supervisory Authority**" means an independent public authority responsible for implementing, interpreting, and/or enforcing any Data Protection Laws.

"**VTEX**" means the VTEX entity which is a party to this DPA, as specified in the section "HOW THIS DPA APPLIES TO CONTRACTOR AND ITS AFFILIATES" above.

"**VTEX Group**" means VTEX and its Affiliates engaged in the Processing of Personal Data.

Without limiting the foregoing, when any term that is defined or used in this DPA is also defined in any Data Protection Law, such defined term shall be interpreted in a manner that is consistent with such Data Protection Law as in effect in the jurisdiction in which the Services are performed and/or in which the applicable Data Subject is located.

2. PROCESSING OF PERSONAL DATA

2.1. **Roles of the Parties**. The parties acknowledge and agree that with regard to the Processing of Personal Data in the context of performance of the Agreement, Contractor is the Controller, VTEX is the Processor and that VTEX will engage Sub-processors pursuant to the requirements set forth in Section 4

"Sub-processors" below. The parties agree that, to the extent VTEX and/or any VTEX Affiliate is acting as Controller in relation to Contractor's individual business contacts' Personal Data, and Contractor is acting as Controller in relation to VTEX's individual business contacts' Personal Data, each act as a separate and independent Controller from Contractor and/or Contractor Affiliates.

2.2. **Contractor's Processing of Personal Data**. Contractor shall, in its use of the Services and provision of instructions, Process Personal Data in accordance with the requirements of applicable Data Protection Laws.

Contractor shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Contractor acquired Personal Data provided to VTEX. Contractor represents and warrants that it has all necessary rights and needed consents from Data Subjects to share the Personal Data with VTEX and for VTEX to Process the Personal Data as contemplated in the Agreement and this DPA. Contractor further represents and warrants that its use of the Services will not violate the rights of any Data Subject that has opted-out from sales or other disclosures of Personal Data, to the extent applicable under the CCPA.

2.3. **VTEX's Processing of Personal Data**. As Contractor's Processor, VTEX and any person acting under its authority or that of a VTEX Affiliate, who has access to Personal Data, shall only Process Personal Data in accordance with Data Protection Laws (as applicable to Processors) and comply with all obligations applicable to Processors under such laws and shall:

(i) Process the Contractor Personal Data in accordance with the Agreement, including for the provision and maintenance of the Services and for the use of the Services by Authorized Users;

(ii) Processing resulting from the use of the Services by Authorized Users; and

(iii) Process the Contractor Personal Data in accordance with reasonable and documented instructions provided by Contractor (e.g., via email or support tickets) that are consistent with the terms of the Agreement;

(individually and collectively, the "**Purpose**")

(iv) Not process that Personal Data except on instructions from the Contractor, unless required to do so by any Data Protection Laws to which the relevant contracted Processor is subject, in which case VTEX or the relevant VTEX Affiliate shall inform Contractor or the relevant Contractor Affiliate of that legal obligation before such Processing, unless that law prohibits such information on important grounds of public interest. When processing Special Categories of Data as defined in Appendix 1 or native Categories of Data with processes that were customized by the Controller or its commissioned actors, VTEX's responsibility is limited to the storage of this data. This DPA and the Agreement are Contractor's complete and final instructions at the time of execution of the DPA for the Processing of Personal Data. Any additional or alternate instructions must be requested separately in writing to VTEX; and

(v) inform Contractor or relevant Contractor Affiliate if, in the VTEX or relevant VTEX Affiliate's opinion, instructions given by the Controller infringe Data Protection Laws.

2.4. **Details of the Processing**. The subject-matter of Processing of Personal Data by VTEX is as described in the Purpose in Section 2.3. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are

further specified in Appendix 1 (Description of the Processing Activities) to this DPA.

3. RIGHTS OF DATA SUBJECTS

3.1. **Data Subject Requests**. VTEX shall, to the extent legally permitted, promptly redirect a Data Subject Request to Contractor if VTEX receives any requests from a Data Subject to exercise the following Data Subject rights under the Data Protection Laws in relation to Personal Data: access, rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, objection to the Processing, or to not be subject to an automated individual decision making (each, a "Data Subject Request"). Taking into account the nature of the Processing, VTEX shall assist Contractor by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of Contractor's obligation to respond to a Data Subject Request under applicable Data Protection Laws. In addition, to the extent Contractor, in its use of the Services, does not have the ability to address a Data Subject Request, VTEX shall, upon Contractor's instructions, provide commercially reasonable efforts to assist Contractor in responding to such Data Subject Request, to the extent VTEX is legally permitted to do so and the response to such Data Subject Request is required under applicable Data Protection Laws. To the extent legally permitted, Contractor shall be responsible for any costs arising from VTEX's provision of such assistance, including any fees associated with provision of additional functionality.

4. SUB-PROCESSORS

4.1. **Appointment of Sub-processors**. Contractor acknowledges and agrees that (a) VTEX's Affiliates may be retained as Sub-processors through written agreement with VTEX and (b) VTEX and VTEX's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services. As a condition to permitting a Sub-processor to Process Personal Data, VTEX (or a VTEX Affiliate acting as Sub-processor) will enter into a written agreement with each Sub-processor containing data protection obligations that provide at least the same level of protection for Personal Data as those in this DPA, to the extent applicable to the nature of the Services provided by such Sub-processor.

4.2. **List of Current Sub-processors and Notification of New Sub-processors**. A current list of Sub-processors engaged by VTEX for the provision of the Services, including the identities of those Sub-processors and their country of location, is available in Appendix 1 to this DPA. Such list may be updated and will remain accessible via https://vtex.com/us-en/privacy-and-agreements/subprocessors/ ("**Sub-processor List**"). VTEX shall maintain an updated List of the Sub-processors before authorized to Process Personal Data in connection with the provision of the applicable Services.

5. SECURITY

5.1. **Controls for the Protection of Personal Data**. VTEX shall maintain appropriate technical and organizational measures for protection of the security, confidentiality and integrity of Personal Data in the context of the provision of the Services. VTEX regularly monitors compliance with these measures. VTEX will not materially decrease the overall security of the Services during a subscription term.

5.2. **Third-Party Certifications and Audits**. VTEX has obtained the third-party certifications and audits set forth in Appendix 2. Upon Contractor's request, and subject to the confidentiality obligations set forth in the Agreement, VTEX shall make available to Contractor (or Contractor's independent, third-party auditor) information regarding the VTEX Group's compliance with the obligations set forth in this DPA in the form of the third-party certifications and audits set forth in Appendix 2t. Contractor may contact VTEX to request an on-site audit of VTEX's procedures relevant to the protection of Personal Data in the context of the provision of the Services, but only to the extent required under applicable Data Protection Laws. Contractor shall reimburse VTEX for any time expended for any such on-site audit at the VTEX Group's then-current rates, which shall be made available to Contractor upon request. Before the commencement of any such on-site audit, Contractor and VTEX shall mutually agree upon the scope, timing, and duration of the audit and any measures to protect the security of third party personal data or VTEX confidential information, in addition to the reimbursement rate for which Contractor shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by VTEX. Contractor shall promptly notify VTEX with information regarding any non-compliance discovered during the course of an audit, and VTEX shall use commercially reasonable efforts to address any confirmed non-compliance.

6. PERSONAL DATA INCIDENT MANAGEMENT AND NOTIFICATION

VTEX maintains security incident management policies and procedures specified in the Appendix 2.

VTEX shall notify Contractor without undue delay of any Personal Data Breach of which VTEX becomes aware as required by Data Protection Laws or the Standard Contractual Clauses, as applicable. VTEX shall provide commercially reasonable cooperation and assistance in identifying the cause of such Personal Data Breach and take commercially reasonable steps to assist in the investigation, containment and remediation, including measures to mitigate its adverse effects, to the extent the remediation is within VTEX's control. VTEX shall document any Personal Data Breach, comprising the facts relating to the Personal Data Breach, its effects and the remedial action implemented by VTEX, as long as the remediation is within VTEX's control.

7. RETURN AND DELETION OF PERSONAL DATA

VTEX shall, upon Contractor's request no later than 30 days prior the termination of the Agreement and subject to the limitations described in the Agreement and the Appendix 2, provide the means for the Contractor to extract a complete copy of all Contractor Personal Data in VTEX's possession or, in the absence of any instructions from the Contractor, securely destroy such Personal Data, and demonstrate through a written certification to Contractor that it has taken such measures, unless applicable law prevents it from returning or destroying all or part of Personal Data or requires storage thereof, in which case VTEX warrants that it will continue to ensure compliance with this DPA and will only process the necessary data to the extent and for as long as required under that applicable law. Contractor acknowledges that VTEX may comply with the above obligation by providing the interfaces necessary to the Contractor to retrieve the Personal Data by its own means. For clarification, data that is not available for self-service retrieval may incur additional charge(s) to be supported by Contractor.

8. CONTROLLER AFFILIATES

8.1. Contractual Relationship. The parties acknowledge and agree that, by executing the DPA in accordance with “HOW TO EXECUTE THIS DPA," Contractor enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Controller Affiliates, thereby establishing a separate DPA between VTEX and each such Controller Affiliate subject to the provisions of the Agreement and this Section 8 and Section 9. The Contractor warrants that it has the power and authority to enter into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Controller Affiliates. Each Controller Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the avoidance of doubt, a Controller Affiliate is not and does not become a party to the Agreement, and is only a party to the DPA. All access to and use of the Services by Controller Affiliates must comply with the terms and conditions of the Agreement and any violation of the terms and conditions of the Agreement by a Controller Affiliate shall be deemed a violation by Contractor.

8.2. Communication. The Contractor that is the contracting party to the Agreement shall remain responsible for coordinating all communication with VTEX under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Controller Affiliates.

8.3. Rights of Controller Affiliates. If a Controller Affiliate becomes a party to the DPA with VTEX, it shall, to the extent required under applicable Data Protection Laws, also be entitled to exercise the rights and seek remedies under this DPA, subject to the following:

8.3.1. Except where applicable Data Protection Laws require the Controller Affiliate to exercise a right or seek any remedy under this DPA against VTEX directly by itself, the parties agree that (i) solely the Contractor that is the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Controller Affiliate, and (ii) the Contractor that is the contracting party to the Agreement shall exercise any such rights under this DPA not separately for each Controller Affiliate individually but in a combined manner for all of its Controller Affiliates together (as set forth, for example, in Section 8.3.2, below).

8.3.2. The parties agree that the Contractor that is the contracting party to the Agreement shall, if carrying out an on-site audit of the VTEX procedures relevant to the protection of Personal Data, take all reasonable measures to limit any impact on VTEX by combining, to the extent reasonably possible, several audit requests carried out on behalf of different Controller Affiliates in one single audit.

9. LIMITATION OF LIABILITY

Each party’s and all of its Affiliates’ liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Controller Affiliates and VTEX, whether in contract, tort or under any other theory of liability, is subject to the ‘Limitation of Liability’ section of the Agreement, and any reference in

such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together.

For the avoidance of doubt, VTEX's and its Affiliates' total liability for all claims from the Contractor and all of its Controller Affiliates arising out of or related to the Agreement and each DPA shall apply in the aggregate for all claims under both the Agreement and all DPAs established under the Agreement, including by Contractor and all Controller Affiliates, and, in particular, shall not be understood to apply individually and severally to Contractor and/or to any Controller Affiliate that is a contractual party to any such DPA.

10. LEGAL EFFECT

This DPA shall only become legally binding between Contractor and VTEX when the formalities steps set out in the Section "HOW TO EXECUTE THIS DPA" above have been fully completed. If Contractor has previously executed a data processing addendum with VTEX, this DPA supersedes and replaces such prior Data Processing Addendum.

11. GOVERNING LAW

As established in the Clause "Governing Law" in the Master Services Agreement.

12. DATA PROCESSING ACTIVITIES

The subject matter of the Processing of the Contractor Personal Data; the duration of the Processing; the nature and purpose of the Processing of the Contractor Personal Data; and the details of the obligations and rights of the Contractor and VTEX are as set out in Appendix 1 of this DPA.

Location, date and signatures on the Order Form - Commercial Proposal

IN WITNESS WHEREOF, this DPA is entered into and becomes a binding part of the Agreement with effect from the DPA Effective Date first set out above.

List of Exhibits

Appendix 1 - Description of the Processing
Appendix 2 - Technical and Organizational Measures

APPENDIX 1 - DESCRIPTION OF THE PROCESSING

A. LIST OF PARTIES

We made available all parties through our website:
https://vtex.com/us-en/privacy-and-agreements/subprocessors/

Contractor has authorized the use of the following service providers:

a. **VTEX ENTITY IDENTIFIED IN THE MASTER SERVICES AGREEMENT**
Role (controller/processor): Processor

b. **VTEX BRAZIL**
Name: VTEX Brasil Tecnologia para E-commerce LTDA
Address: Avenida Brigadeiro Faria Lima, nº 4.440, 10º andar, Vila Olímpia, CEP 04538-132, inscrita no CNPJ/MF sob o n. 05.314.972/0001-74
Role (controller/processor): Subprocessor

c. **AWS**
Name: Amazon Web Services Inc.
Address: United States
Role (controller/processor): Subprocessor

B. DESCRIPTION OF TRANSFER

Subject matter and duration of the processing of the Personal Data

The subject matter of the Processing of the Contractor Personal Data are as set out in the Agreement and this DPA. Processing operations are carried out in the context of the performance of the Agreement for the provision and management of the Services by VTEX to the Contractor.

The duration of the Processing is aligned to that of the Agreement.

Nature of the processing, purpose(s) of the data transfer and further processing

The Personal Data transferred will be processed for the purposes of the Services to be provided under the Agreement and any Order Form - Commercial Proposal and may be subject to the following processing activities:

- storage and other processing necessary to provide, maintain, and update the Services provided to the Contractor;
- to provide Contractor maintenance and technical support ; and
- disclosures in accordance with the Agreement, as compelled by law.

There is no further processing other than transfers to subprocessors.

The categories of Data Subject to whom the Contractor Personal Data relates

The categories of Data Subject may include some or all of the following:

- Contractor's personnel;
- Contractor's end-users (clients)

The types of Personal Data to be processed: IP; navigation Information such as cookies; cart information; order information; email; phone number; address; ID number, gift card history; name; order history; navigational information; unused cart; conversations; sessions passwords; generated tokens; sessions.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Contractor may submit special categories of Personal Data to the VTEX as the case may be, through the Services, the extent of which is determined and controlled by the Contractor in compliance with applicable Data Protection Laws.

The obligations and rights of the Contractor and VTEX.

The details of the obligations and rights of the Contractor and VTEX are as set out in the Agreement and this DPA.

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

Data is transferred on a continuous basis for the purposes of the Services to be provided under the Agreement and any Order Form - Commercial Proposaldescribed under Article 13 of the DPA.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

To be mutually agreed between Contractor and VTEX, in accordance with applicable laws governing privacy, e-commerce transactions and tax laws.

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

VTEX hires Amazon Web Services Inc. and Microsoft Inc. (Azure) as Cloud Service Providers for hosting purposes for the duration of the Master Services Agreement executed by and between VTEX and Contractor.

APPENDIX 2 - TECHNICAL AND ORGANIZATIONAL MEASURES INCLUDING TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

VTEX has implemented and will maintain appropriate technical and organizational measures to protect the personal data against misuse and accidental loss or destruction as set forth in VTEX Privacy and Security Policies.

VTEX's current technical and organizational measures are set forth below.

As mentioned above, below is a non-exhaustive list of points that are currently implemented in VTEX with a focus on data protection and security considering the triad of: IT, Security and Privacy.

1. Awareness and Training
    a. The company has training cycles for different levels of employees with a focus on privacy and security. VTEX will also have training focused on good practices in secure development.
2. Password protection
    a. VTEX currently saves passwords in one way: HashVector(Main Algorithm used here is PBKDF2 with SHA256).
3. Anti-virus Policy
    a. The IT team has a policy of keeping all of its staff computers with antivirus.
4. Data classification
    a. VTEX has an information classification policy to understand what type of protection each type of data needs.
5. Vulnerability management
    a. VTEX performs regular threat and vulnerability reviews of the platform and operation processes. Risk identification triggers the improvement of our monitoring and notification systems to handle their eventual materialization, be it by notifying personnel who are able to deal with it or by triggering automated actions that can mitigate or eliminate them. In point 15 of the appendix we bring the functioning of our pentests in detail.
6. Certifications
    a. As defined by industry standards, company certifications will typically cover a period from January to December, December being the month to renew the certification for that current year. Hence, when we speak of the current certifications we have, we are referring to those we have maintained until the last possible period. The certifications VTEX has maintained until the last applicable period, therefore, are:
        i. SOC 1 - Type 2: A report covering internal controls over financial reporting systems;
        ii. SOC 2 - Type 2: A report covering Security, Availability, Integrity, Confidentiality, and Privacy;
        iii. SOC 3 - A public report of Security, Availability, Integrity, Confidentiality and Privacy Controls;
        iv. PCI - A validation of controls around cardholder data to reduce credit card fraud.
        v. All of these certifications are available under the Compliance section on the VTEX Trust Hub (https://vtex.com/us-en/trust/)
7. VTEX measures to ensure the security of the data

   a. The data in transit is always encrypted, in addition to that VTEX have in-house solutions for building application security, and also carry out test cycles with third-party companies in order to improve our solutions in addition to the use of backup policies and evaluation of possible failures and incident reviews. Finally, external audits ensure that most of these flows: Data anonymization, secure processing, among others, are respected and carried out.

8. How we address Data Backup and Redundancy
   a. Most of the data handled by VTEX is stored on AWS services using managed services such as S3, RDS and DynamoDB. All of those services provide AWS managed backup infrastructure that is used by VTEX. The AWS platform is a reference in the cloud computing industry and holds important certifications such as: ISO 27001, PCI DSS, CSA, NIST and many others. (To see a list of detailed certifications, access: https://aws.amazon.com/en/compliance/programs/)
9. Disaster Recovery and Incident Recovery
   a. VTEX's Disaster and Incident Recovery Plan consists of internal policies and procedures that VTEX will follow in case of service disruption. This could happen because of a natural disaster, or as a result of technological failure or human factors. The goal is to restore the affected business processes as quickly as possible, whether by bringing the disrupted services back online or by switching to a contingency system.
   b. The scope of this plan is VTEX Cloud Commerce Platform, including: (i) all services that constitute the solution; (ii) all business processes that support it or its operation; (iii) all business processes that support VTEX's clients who depend on VTEX Cloud Commerce Platform;
   c. VTEX's Disaster and Incident Recovery Plan is fully supported and implemented by automated processes that are triggered based on also automated monitoring and notification tools.
   d. Recovery Time Objective (RTO): is the maximum amount of time that should be allowed to elapse before normal services are resumed. Service downtime may be related to application disruption, data corruption or data loss, data server failure, or AWS Availability Zone or Region disruption. VTEX's Disaster and Incident Recovery Plan is tested at least annually, in order to see that it will be effective at any moment it is needed.
   e. External stakeholders are notified through the status page (https://status.vtex.com): the status page is publicly available to anyone interested in seeing VTEX True Cloud CommerceTM platform current health status. It is also used as a notification tool for planned maintenance, which is not in the scope of the DRP.
10. Private Data Encryption
   a. As of today, and following our commitment to compliance with the Data Privacy Laws, VTEX guarantees encryption according to what the privacy and compliance regulations surrounding PII require. For example, our Payments Product is PCI compliant and implements data encryption and key rotation according to the PCI DSS standards. On top of this, VTEX has ongoing engineering projects to implement encryption and isolation of PII data as well as to implement audit logging in a multitude of applications on top of those of ours that already offer it.
11. Data Storage at VTEX
   a. VTEX's hosting provider is AWS, the world's leading provider of cloud computing services, and the data is stored in the AWS region of Northern Virginia, United States. One of the key pillars of AWS is "Security is Job Zero", a statement that proves that information security is placed before anything else in AWS with which VTEX strongly identifies.

12. Data Transmission
    a. All incoming traffic into VTEX's network is protected using TLS 1.2 technology over http.
13. Customer and Network Segregation
    a. Production network is completely isolated from external networks. VTEX employees responsible for production environments operation may need eventual VPN connection to access the production network.
14. Physical Security and Environmental Protection
    a. The physical assets utilised by VTEX are provided by AWS as part of the service provided by them.
15. Pentest policies

    Due to the nature of VTEX's business, we are building a policy of performing quarterly penetration tests, currently the tests take place annually. In addition, several clients independently evaluate our platform, so we are always audited both externally and internally.

16. Controls for sub processors

VTEX has a sub processor analysis questionnaire that includes some security questions to analyse the potential risks of each relationship. The methods used to assess the security of third parties are selected by considering the type and severity of risks in these relationships, the adequacy and relevance of the details that can be obtained about security processes and controls. More specifically, AWS, listed as a subprocessor in Appendix 1, holds security and privacy certifications ISO 27017:2015 and ISO 27018:2014, which are subsets based on ISO 27001:2013, the most comprehensive security standard.

***