VTEX Global Data Processing Addendum

This Global Data Processing Addendum (**"DPA"**) serves as Appendix 2 to the Master Services Agreement available at https://vtex.com/us-en/agreements, entered into by Customer and VTEX. Together, the Master Services Agreement ("MSA"), the Order Form - Commercial Proposal and this DPA, are referred to as the "**Agreement**".

In consideration of the mutual promises set out in this DPA, Customer and VTEX agree as follows:

1 Types of Data & Purposes of Processing.

Outlined below are the types of personal data, categories of data subjects, purposes, and the points and methods of personal data collection that will be processed.

Personal Data	*Personal identifiers:* - First, middle and/or last name, alias, signature, email, address, or phone number - Government-issued ID or tax enrollment number (e.g., CPF, RUT, passport number, driver's license number) *Online data:* - Unique personal identifier or online identifier (e.g., cookie and/or device ID or IP address) - access information (e.g., username and/or encrypted password) - Activity information (e.g., browsing history, search history, cart information, orders history, gift card history, support history, or interactions with content or ads) - Inferences derived from preferences and behavior *Payment information:* - credit card number or debit card number (all encrypted according to PCI-DSS standards)
Who Data Pertains To (Categories of Data Subjects)	- Customer's end consumers (e.g., shoppers, site visitors, or subscribers) - Customer's employees
Purposes For Processing Data	- Performing Services under the Contract (e.g., maintaining or servicing accounts, providing customer service, fulfilling orders and transactions, processing payments, providing advertising or marketing services according to Customer's instructions) - Auditing related to a current interaction (e.g., counting and verifying ad impressions) - Detecting, preventing, and investigating security incidents, fraudulent, or illegal activity - Debugging errors that impair functionality and maintaining or enhancing the availability of the Services - Product improvement and development - Performing data analytics, aggregation and/or de-identification, including to develop insights for the benefit of Customer
Point of Data Collection	- Customer website, mobile app, or similar digital service
Method of Data Collection	- Forms directly completed by data subject (e.g., newsletter sign up, survey, entry form) - Cookies, pixels, tags, SDKs, and similar technologies

2 Definitions and Interpretation.

Any terms in capitalised letters are defined either: (i) in the applicable **Data Protections Laws**, such as "**Data Controller**", "**Personal Data**", "**Data Processor**" and "**Subprocessor**"; (ii) by the meanings given to them in the MSA; or (iii) in this clause. For the purposes of this DPA, "**Personal Data**" means any information that relates to an identified or identifiable natural person, protected under applicable Data Protection Laws, provided by Customer, in the position of Data Controller, to VTEX, in the position of Data Processor, in the context of performance of the Agreement.

"**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with the Customer. "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.

"**Authorised Users**" means any person who is given access by Customer to the VTEX Platform environment in accordance with the requirements set out in the Agreement.

"**Customer**" means the entity identified in the Order Form - Commercial Proposal that is signing this DPA on behalf of itself and on behalf of any Customer Affiliates.

"**Customer Affiliate**" means any of Customer's Affiliate(s) that are permitted to use the Services pursuant to the MSA between Customer and VTEX. If and to the extent VTEX processes Personal Data on behalf of such Affiliate(s), the Affiliate qualifies as the Controller.

"**Customer Personal Data**" means any Personal Data relating to Authorised Users received for the purposes of authorising access to the Services, or the representatives of the Customer or Affiliates in connection with execution and administration of the Agreement, which Personal Data VTEX processes as a controller.

"DPF" means the mechanisms for personal data transfers to the United States from the European Union / European Economic Area, the United Kingdom (and Gibraltar), and Switzerland, according to the EU-U.S. Data Privacy Framework (**"EU-U.S. DPF"**), the UK Extension to the EU-U.S. Data Privacy Framework (**"UK Extension to the EU-U.S. DPF"**), and the Swiss-U.S. Data Privacy Framework (**"Swiss-U.S. DPF"**), in reliance on the European Commission's adequacy decision effective July 10, 2023.

"Data Protection Laws" means all laws, regulations by data protection supervisory authorities, and court / administrative orders in any jurisdiction to which Customer is bound in connection with the Services provided under the Agreement, including those concerning: (a) privacy; (b) the security, loss or misuse of data, (c) marketing and commercial advertisements; and (d) the responsible use and protection of data.

"SCC" means sections I, II, III and IV (as applicable) to the extent they reference Module Two (Controller-to-Processor) within the Standard Contractual Clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as currently set out at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj, as amended, superseded or is required to be implemented in connection with the SCC from time to time.

"**UK SCC**" means the SCC transposed into United Kingdom national law by operation of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 ("**UK GDPR**"), pursuant to Article 46 of the UK GDPR.

"Security Breach" means the accidental or unauthorized access, loss, alteration, or disclosure, of processed Personal Data. A Security Breach includes without limitation, a "personal data breach", or other similar term as defined in Data Protection Laws.

"**Supervisory Authority**" means an independent regulatory authority responsible for the enforcement of Data Protection Laws.

3 Processing Details.

3.1 **Roles of the Parties.** For the purposes of this DPA, the Data Controller is the Customer (as defined in the Order Form - Commercial Proposal) and any Customer Affiliate; the Data Processor is VTEX (as defined in the Order Form - Commercial Proposal); and the Subprocessors are AWS (Northern Virginia Region - USA) and VTEX Brasil Tecnologia para E-commerce Ltda.

3.2 **International Data Transfers**. When VTEX processes Personal Data of Data Subjects located in the EEA, Switzerland, or the United Kingdom in a country that has not received an adequacy decision from the European Commission or Swiss or UK authorities, as applicable, such transfer shall take place on the basis of VTEX's certification under the DPF. If the DPF is declared invalid, or if VTEX fails to re-certify for DPF, then the transfer of Personal Data will be subject to the SCC or UK SCC, as applicable, which the parties agree will be incorporated by reference into this DPA. The parties agree that, with respect to the elements of the SCCs and the UK SCC that require the parties' input, Schedules 1-4 contain all the relevant information.

3.3 **Scope of Processing.** The Agreement is Customer'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. VTEX shall at all times: (i) process Personal Data only for the purpose of providing the Services to Customer as described in the table on pages 1 and 2 and Schedules 1-4 for the purposes of the SCC; (ii) in accordance with Customer's documented instructions; and (iii) not process Personal Data for its own purposes or those of any third party. VTEX shall promptly notify Customer in writing, unless prohibited from doing so under Data Protection Laws or other applicable laws, if it: (a) becomes aware or believes that any data processing instruction from Customer violates Data Protection Laws, or it is unable to comply with Customer's data processing instructions; and/or (b) is unable to comply with the terms of the Agreement as they relate to or govern the processing and/or the security of Personal Data.

3.4 **Mutual Obligations.** To the extent applicable to each party's performance or use of the Services, as the case may be, including to the extent each party collects Personal Data directly from individuals, each party represents and warrants that it will: (i) comply with Data Protection Laws with respect to any Personal Data received, collected, processed, shared, or stored by such party, including any applicable industry self-regulatory guidelines, frameworks, or codes; (ii) maintain conspicuous consumer-facing privacy notice, cookies disclosures, and/or other legally required statement, which accurately disclose all applicable data collection, use, sharing, disclosure, and security practices; (iii) obtain any required permissions and opt-in or opt-out consents from individuals and respect such consumer choices; (iv) establish and maintain lawful processes for the exercise of data subject rights and honor any valid rights requests regarding Personal Data and Customer's Personal Data, as applicable to each party; and (v) ensure that individuals with access to Personal Data are subject to an appropriate contractual or statutory obligation of confidentiality.

4 Customer's Obligations.

4.1 **Lawful basis**. Customer has sole responsibility for the accuracy, quality, and lawfulness of Personal Data and the means by which Customer acquired the Personal Data provided to VTEX. Customer warrants that it has all lawful basis to share the Personal Data with VTEX and for VTEX to process the Personal Data as contemplated in the Agreement.

5 VTEX's Obligations.

5.1 **Regional Schedules.** VTEX agrees to include additional obligations according to the laws in force at the country and/or territory applicable to Customer, as established in the Order Form. Such obligations are set forth in the CCPA Schedule, LATAM Schedule, GDPR Schedule, and other Schedules, each to the extent applicable to VTEX's processing of Personal Data according to the applicable law and territories set forth in the MSA. To the extent there are any conflicts between a Schedule and the main body of this DPA, the Schedule shall prevail.

5.2 **Data Subject Rights and Cooperation.**

5.2.1 VTEX shall cooperate with Customer to enable Customer to respond to any valid requests, complaints, or other communications from individuals, regulatory or judicial bodies, or other relevant entities, relating to the processing of Personal Data (**"Request"**), including Requests from individuals to exercise their rights under Data Protection Laws. In the event that such Request is made directly to VTEX, VTEX shall notify the Customer in writing within 2 (two) business days.

5.2.2 If VTEX receives a subpoena, court order, warrant, or other legal demand from a third party (including law enforcement or other public or data protection supervisory authorities) seeking the disclosure of Personal Data, to the extent not prohibited by law, VTEX shall promptly notify Customer in writing of such request, and reasonably cooperate with Customer if it wishes to limit, challenge, or protect against such disclosure.

5.3 **Sub-processors and Employees.** Customer acknowledges and generally agrees that (a) VTEX's Affiliates are Sub-processors under this DPA specially for technical support purposes and (b) VTEX and VTEX's Affiliates may engage third-party Sub-processors, such as AWS, Northern Virginia Region, USA, in connection with the provision of the Services. A current list of Sub- processors engaged by VTEX for the provision of the Services is available in https://vtex.com/us-en/privacy-and-agreements/subprocessors/ ("**Sub-processors List**"). VTEX will contractually impose the same level of protection or higher to the Sub-processors for processing Personal Data as provided for in this DPA. VTEX shall ensure that employees authorized to process Personal Data are: (i) obligated to keep Personal Data confidential; and (ii) properly trained in the processing of Personal Data under applicable Data Protection Laws.

5.4 **Data Protection Impact Assessment.** To the extent Customer does not otherwise have access to the relevant information, VTEX will provide Customer with reasonable cooperation and assistance needed to carry out a data protection impact assessment, or any similar assessment required by Data Protection Laws, related to Customer's use of the Services, where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons.

5.5 **Security Measures & Compliance Audits.**

5.5.1 VTEX will: (i) implement appropriate technical and organizational security measures to protect Personal Data from a Security Breach using measures appropriate to the risks that are presented by the nature of the processing of Personal Data (and such measures will meet or exceed those identified in Schedule 3); (ii) regularly monitor compliance with such measures; (iii) upon request, make available to Customer a copy of its then most recent third-party audit results or certifications related to such measures to the extent VTEX makes them generally available to its customers; and (iv) timely respond to Customer's annual VTEX information security and privacy questionnaire. If, in Customer's reasonable determination, the information provided under (iii) and (iv) are inadequate or in the event of a Security Breach, VTEX agrees to allow for an independent third-party audit or inspection (provided that such audit or inspection will be performed by an auditor mutually agreed upon the parties, at Customer's sole expense and no more than one time a year except if the audit or inspection occurs in response to a Security Breach). Before the commencement of any such independent audit or inspection, Customer and VTEX will mutually agree upon the scope,

timing, and duration of the audit or inspection and VTEX will provide reasonable assistance and cooperation to enable such audit or inspection. Where required by Data Protection Laws, VTEX will maintain a comprehensive written plan and/or policy related to implementing such measures and provide a summary of such plan and/or policy to Customer upon request.

5.5.2 **Audits.** Customer may audit VTEX's compliance with the Technical and Organizational Measures relevant to Personal Data processed by VTEX ("**Customer Audit**") on request only if:

(a) VTEX has not provided sufficient evidence of its compliance with the Technical and Organizational Measures set forth in Schedule 3, 3.3, e.g. ISO 27001, SOC 2 - Type 2, or other standards as defined in the certifications ("**Audit Reports and Certifications**"); or

(b) a Personal Data breach has occurred; or

(c) an audit is formally requested by Customer's data protection authority; or

(d) Data Protection Law sets out a direct audit right.

5.5.3 **Audit Specifications.** Prior to initiating a request for audit, Customer shall review VTEX's Audit Reports and Certifications. Customer or its independent third party auditor (reasonably acceptable by VTEX, acting on behalf of Customer) shall provide at least 60 days' advance notice of any Customer Audit unless Data Protection Law or a Customer's data protection authority requires shorter notice. The start date, timeframe and scope of any Customer Audit shall be mutually agreed upon between the parties, acting reasonably. Unless Data Protection Laws require more frequent audits, the frequency of a Customer Audit shall not exceed once every 12 months. VTEX resources to support Customer Audits shall be limited to a maximum equivalent of 3 business days, during VTEX's normal business hours, not disrupt VTEX's normal business operations and be subject to VTEX's confidentiality requirements. Customer will share any report resulting from a Customer Audit to VTEX.

5.5.4 **Audit Costs**. In the event an audit is conducted out of the specifications provided on 5.5.3, then Customer shall bear all reasonable costs of such audit and any required work by VTEX, at the VTEX's then-current rates. If a Customer Audit reveals a material breach by VTEX of this DPA, then VTEX will run its own audit, to confirm such material breach. In that case, remediation proceedings set forth in the Agreement will apply.

5.6 **Security Breach.**

5.6.1 In the event of a Security Breach, VTEX will:

(i) Promptly, and in no event later than seventy-two (72) hours of becoming aware of such Security Breach, inform Customer and provide written details of the Security Breach, including, if applicable, the type of Personal Data affected and the identity of impacted person(s) as soon as such information becomes known or available to VTEX;

(ii) VTEX will provide timely information and cooperation as Customer may require to fulfill its data breach reporting obligations under Data Protection Laws or to comply with or respond to any inquiries by a data protection authority or any lawsuit arising from the Security Breach, except when such information includes third party confidential information;

(iii) Investigate the Security Breach and perform a root cause analysis;

(iv) Take such measures and actions as are appropriate to remedy or mitigate the effects of the Security Breach and keep Customer up-to-date about developments in connection with the Security Breach; and

(v) In case the root cause analysis demonstrates that the Security Breach was exclusively caused by VTEX, VTEX will reimburse Customer for any reasonable costs and expenses incurred in connection with a Security Breach, including the cost of notifications to individuals and identity theft monitoring and resolution services (including credit monitoring services) to affected parties, in the terms of clause 6. Liability.

5.6.2 The content and provision of any notification, public/regulatory communication, or

press release concerning the Security Breach will be solely at Customer's discretion, except as otherwise required by Data Protection Laws or reference is made to VTEX in such announcements – in such case, VTEX must approve the content in writing and advance to any announcement.

5.7 **Deletion and/or Transfer**. VTEX will, at any time but no later than the Agreement termination, provide the means for the Customer to extract a complete copy of all Personal Data in VTEX's possession or, in the absence of any instructions from the Customer, securely destroy such Personal Data. Customer acknowledges that VTEX may comply with the above obligation by providing the interfaces necessary to the Customer to retrieve the Personal Data by its own means, at Customer's own administrative environment on the VTEX Platform. This option will remain available, as default, until the termination date of the Agreement.

6 Liability.

6.1. 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 Customer Affiliates and VTEX, whether in contract, tort or under any other theory of liability, is subject to the '**VTEX LIMITATION OF LIABILITY**' section of the MSA. 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 MSA. In particular, the aggregate of all claims shall not be understood to apply individually and severally to Customer and/or to any Customer Affiliate that is a contractual party to the MSA. VTEX shall be liable for the acts and omissions of its Sub-processors to the same extent VTEX would be liable if performing the services of each Sub-processor directly under the terms of this DPA.

7 Governing Law & Dispute Resolution

As established in the Clause "**GOVERNING LAW & ARBITRATION**" in the Master Services Agreement.

As an exception to the foregoing, in respect of UK Restricted Transfers only, "**governing law**" shall be the laws of England and Wales.

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.

Schedule 1: International Transfers - Description of the Processing and Subprocessors

Processing Activity	**Customer discloses Customer Personal Data to VTEX to provide, operate, and maintain VTEX Services**	**Customer contacts VTEX for technical support**	**Customer processes end-user / shoppers' Personal Data on VTEX Services**
Types of Data & Purposes of Processing	Please refer to "Types of Data & Purposes of Processing" in the DPA.		

Status of the Parties	VTEX and Customer are Data Controllers	VTEX and Customer are Data Controllers	VTEX is a Data Processor Customer is a Data Controller
Categories of Personal Data Processed	Account registration, user content, communication, tracking technologies, usage of Services, and third party accounts (according to integrations chosen by Customer).	Account registration, user content, communications, usage of Services, and third party accounts (according to integrations chosen by Customer).	As determined by Customer (please refer to "Types of Data & Purposes of Processing" Section on the DPA).
Categories of Sensitive Personal Data Processed	None	None	As determined by Customer
Frequency of Transfer	Continuous	Continuous	As determined by Customer
Applicable SCC Module	Module 1	Module 1	Module 2
Subprocessors	For a complete list, please refer to https://vtex.com/us-en/privacy-and-agreements/subprocessors/ **Data Exporter:** Customer appointed in the Agreement **Data Importer:** VTEX Entity appointed in the Agreement **Subprocessor 1**: VTEX Brasil Tecnologia para E-commerce Ltda. for technical support purposes **Subprocessor 2**: Amazon Web Services Inc., Northern Virginia Region, USA.		

Schedule 2: Information for SCC - Module 1

1. Retention Periods

VTEX retains Personal Data it collects as a Controller for as long as VTEX has a business purpose for it or for the longest time allowable by applicable law.

2. SCCs

2.1. For the purposes of the Standard Contractual Clauses:

Clause 7, Module 1: The parties agree that the docking clause shall not apply.
Clause 11(a), Module 1: The parties do not select the independent dispute resolution option.
Clause 17, Module 1: The parties select Option 1. The Member State is as stated in the venue clause of the Agreement.
Clause 18(b), Module 1: The Parties agree that those shall be the courts as stated in the venue clause of the Agreement.

Annex I (A): The data exporter is Customer. The data importer is VTEX. Contact details for Customer is the email address(s) designated by Customer in Customer's VTEX account. Contact detail for VTEX is dpo@vtex.com, or as stated in the Agreement.

Annex I (B): The parties agree that Schedule 1 describes the transfer.

Annex I (C): The competent supervisory authority is the supervisory authority of the ICO.

Annex II: The Parties agree that Schedule 3, Section 3.3. describes the technical and organizational measures applicable to the transfer.

2.2. For purposes of the UK Addendum:

Table 1: The data exporter is Customer. The data importer is the VTEX Entity appointed in the Agreement. Contact details for Customer is the email address(s) designated by Customer in Customer's VTEX account. Contact detail for VTEX is dpo@vtex.com, or as stated in the Agreement.

Table 2: The Parties select the checkbox that reads: "Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum", and the accompanying table shall be deemed completed according to the Parties' preferences outlined in Schedule 2, Section 2.1 above.

Table 3: Table 3 shall be completed with the information set forth in Schedule 2, Section 2.1 above regarding Annex I(A), Annex I(B), and Annex II.

Table 4: The Parties agree that the data importer may terminate the UK Addendum as set out in Section 19 of the UK Addendum.

UK IDTA Addendum

Table 1: Please refer to the Agreement.

Table 2: UK country's law that governs the IDTA and Primary place for legal claims to be made by the Parties: England and Wales. Status of the Exporter and the Importer: Please refer to Schedule 1. Whether UK GDPR applies to the Importer: Please refer to the Agreement. Linked Agreement and Term: Please refer to the Agreement. Ending the IDTA before the end of the Term: the Parties cannot end the IDTA before the end of the Term unless there is a breach of the IDTA or the Parties agree in writing. Ending the IDTA when the Approved IDTA changes: Importer. Can the Importer make further transfers of the Transferred Data: Please refer to Schedule 1. Specific restrictions when the Importer may transfer on the Transferred Data: Please refer to Schedule 1. Review Dates: each time there is a change to the Transferred Data, Purposes, Importer Information, TRA or risk assessment.

Table 3: Please refer to Schedule 1.

Table 4: Please refer to section 3.3. Technical and Organizational Measures to Ensure the Security of the Data ("TOMs")

Schedule 3: Information for SCC - Module 2

1. Subprocessors

VTEX uses Subprocessors when it acts as a Processor. Customer authorizes VTEX to use these Subprocessors consistent with Section 5.3. Sub-processors are available on our **Sub-processor List**.

2. Retention Periods

VTEX retains Personal Data it collects or receives from Customer as a Processor for the duration of the Agreement and is consistent with its obligations in this DPA.

3. Information for International Transfers

3.1. For the purposes of the Standard Contractual Clauses:

Clause 9, Module 2(a): The parties select Option 2. The time period is 30 days.
Clause 11(a): The parties do not select the independent dispute resolution option.
Clause 17, Module 2: The parties select Option 2. The Member State of the data exporter is the EU Member State Customer is located in.
Clause 18(b), Module 2: The Parties agree that those shall be the courts of the EU Member State appointed in the Agreement.

Annex I (A): The data exporter is Customer. The data importer is the VTEX Entity appointed in the Agreement. Contact details for Customer is the email address(s) designated by Customer in Customer's VTEX account. Contact detail for VTEX is dpo@vtex.com, or as stated in the Agreement.

Annex I (B): The parties agree that **Schedule 1** describes the transfer.

Annex I (C): The competent supervisory authority is the supervisory authority as appointed by Customer who acts as data exporter.

Annex II: The parties agree that Schedule 3, Section 3.3 describes the technical and organizational measures applicable to the transfer.

3.2. For the purposes of UK Addendum:

Table 1: The data exporter is Customer. The data importer is the VTEX Entity appointed in the Agreement. Contact details for Customer is the email address(s) designated by Customer in Customer's VTEX account. Contact detail for VTEX is dpo@vtex.com or as provided in the Agreement.

Table 2: The Parties select the checkbox that reads: "Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum", and the accompanying table shall be deemed completed according to the Parties' preferences outlined in **Schedule 3, Section 3.1 above**.

Table 3: Table 3 shall be completed with the information set forth in (i) **Schedule 3, Section 3.1 above** regarding Annex I(A), Annex I(B), Annex II and (ii) Schedule 3, Section 1 above regarding Annex III.

Table 4: The Parties agree that data importer may terminate the UK Addendum as set out in Section 19 of the UK Addendum.

UK IDTA Addendum

Table 1: Please refer to the Agreement.

Table 2: UK country's law that governs the IDTA and Primary place for legal claims to be made by the Parties: England and Wales. Status of the Exporter and the Importer: Please refer to Schedule 1. Whether UK GDPR applies to the Importer: Please refer to the Agreement. Linked Agreement and Term: Please refer to the Agreement. Ending the IDTA before the end of the Term: the Parties cannot end the IDTA before the end of the Term unless there is a breach of the IDTA or the Parties agree in writing. Ending the IDTA when the Approved IDTA changes: Importer. Can the Importer make further transfers of the Transferred Data: Please refer to Schedule 1. Specific restrictions when the Importer may transfer on the Transferred Data: Please refer to Schedule 1. Review Dates: each time there is a change to the Transferred Data, Purposes, Importer Information, TRA or risk assessment.

Table 3: Please refer to Schedule 1.

Table 4: Please refer to section 3.3. Technical and Organizational Measures to Ensure the Security of the Data ("TOMs")

3.3. Technical and Organizational Measures to Ensure the Security of the Data ("TOMs")

The Data Importer 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.

The Data Importer'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. VTEX provides recurring training cycles, including both general and role-specific sessions, with a strong emphasis on privacy and security. VTEX offers specialized training on secure development practices, aligned with our security certifications.

2. Password protection
    a. Passwords are hashed using PBKDF2 based on SHA-256. During this process, only the resulting hash value is stored, ensuring that the original passwords remain secure and are not directly accessible.
    b. Merchants can choose to enforce password expiration after a specific period for Admin users.
    c. Merchants can also choose to integrate an external identity provider, allowing them to define their own customized password policies.

3. Authorization and access control

VTEX efficiently manages logical access, ensuring precise control and monitoring of access permissions for systems and data. Our practices adhere to security policies, including measures like the principle of least privilege and segregation of duties. Users are granted access only to

that which is strictly necessary for their roles, reducing the risk of exposing sensitive information and bolstering the security of systems and data.

4. Endpoint Security
    a. VTEX uses a comprehensive approach to mitigate cyber attacks, employing measures such as advanced antivirus, firewalls, and content filters to block malware. Our platform includes protection against DDoS (Distributed Denial of Service) attacks and other threats.
    b. VTEX also utilizes monitoring tools to ensure comprehensive security of endpoints.

5. Data classification
    a. VTEX has an information classification policy to determine the appropriate level of protection required for each type of data.

6. Logs

All operations on the platform are automatically logged. Platform errors are logged in Security Information and Event Management software, accessible to the VTEX team for product analysis and improvement purposes.

7. Vulnerability management
    a. VTEX conducts regular threat and vulnerability assessments of our platform and operational processes. Identified risks prompt enhancements to our monitoring and notification systems, enabling us to manage potential issues effectively—whether through alerting relevant personnel or initiating automated actions to mitigate or eliminate them. For a detailed explanation of our penetration testing procedures, please refer to point 14 in the appendix.

8. Certifications
    a. According to industry standards, company certifications generally cover the period from January to December, with December marking the start of the renewal process for the upcoming year. Therefore, when we refer to our current certifications, we mean those that have been maintained through the most recent applicable period. The certifications that VTEX has upheld through this period are as follows:"
        i. ISO 27001: An international standard for information security management systems.
        ii. SOC 1 - Type 2: A report covering internal controls over financial reporting systems.
        iii. SOC 2 - Type 2: A report covering Security, Availability, Integrity, Confidentiality, and Privacy.
        iv. PCI: A validation of controls around cardholder data to reduce credit card fraud.

All of these certifications can be requested from VTEX at any time and are available under the Compliance section on the VTEX Trust Hub (https://vtex.com/us-en/trust/).

9. How VTEX addresses Data Backup and Redundancy
    a. 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/)

10. Business Continuity Plan and Disaster Recovery Plan

a. VTEX has a comprehensive Disaster Recovery Plan, which includes internal policies and procedures designed to address service disruptions. This plan aims to restore affected components as quickly as possible. To ensure its effectiveness, VTEX conducts regular tests of this plan."
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 Recovery Plan is supported and implemented by automated processes that are triggered based on also automated monitoring and notification tools. Additionally, a specialized team oversees these processes and monitors their performance to ensure the plan's effectiveness and responsiveness.
d. 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.

11. Private Data Encryption
    a. VTEX guarantees encryption according to what the privacy and compliance regulations surrounding PII require. Payments Modules are PCI compliant and implements data encryption and key rotation according to the PCI-DSS standards. 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.

12. 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.

13. Data Transmission
    a. All incoming traffic into VTEX's network is protected using TLS 1.2 (or higher) technology over http.

14. Pentest policies
    a. Due to the nature of VTEX's business, we have established a policy of conducting penetration tests at least semiannually. Additionally, In addition, our platform is regularly evaluated by clients, partners, and independent auditors, ensuring ongoing external and internal scrutiny.

    b. Merchants are encouraged to share the pentest reports and vulnerability notifications with VTEX, allowing our Security team to promptly address any potential issues identified.Penetration tests must be previously scheduled with VTEX. Any test conducted autonomously without prior notice to VTEX will be considered an unauthorized action attempt.

15. Third Party Risk Assessment

VTEX has a comprehensive process for evaluating our suppliers to ensure they meet our security and risk management standards. We utilize a detailed subprocessor assessment questionnaire, which includes security-related questions to evaluate potential risks associated with each supplier relationship. Suppliers deemed to present unacceptable risks are either excluded from joining our ecosystem or are contractually obligated to implement a corrective action plan if necessary. For example, AWS, listed as a subprocessor in Schedule 1, maintains security and privacy certifications

ISO 27017:2015 and ISO 27018:2014, which are subsets of ISO 27001:2013, the most rigorous security standard available.

16. Security incident response

VTEX has a formal protocol for security incident response that covers the essential stages of the process: preparation, incident identification, containment, eradication, recovery and post-incident. This procedure also includes an integrated communication plan that is applied at all stages of the response.

***