DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**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**".

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

By signing this addendum, the Contractor enters into this DPA on behalf of itself and, to the extent that the applicable Data Protection Laws require so, on behalf of any Contractor Affiliate (as defined below) that is a third-party beneficiary under 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 Processing of Personal Data.

HOW TO EXECUTE THIS DPA?

1. This DPA consists of two parts: the main body of the DPA, and its 3 appendices and Appendix):
   - **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 organisational Measures**
   - **Appendix 3: EU Standard Contractual Clauses (Module 2) to be used globally**

2. The Data Protection Laws (as defined below) in certain jurisdictions may require the obligations in this DPA and its Appendixes to be supplemented by additional or alternative provisions to ensure the compliance with the respective Data Protection Laws ("Special Terms"). The provisions of this DPA shall also be interpreted in accordance with any Special Terms identified in Exhibit A as applicable to the respective jurisdiction.

3. The Contractor declares to be aware of the clauses foreseen 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 capitalised letters that are not defined below or otherwise in this DPA or in the applicable Data Protections 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.

"**Authorised Users**" means any person authorised by VTEX in writing to have control over VTEX Platform environment and any person who is given access by Contractor to 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. For the purposes of this DPA, the Controller is the Contractor (as defined in the Agreement) and/or any Contractor Affiliate.

"**Contractor Affiliate**" means any of Contractor's Affiliate(s) (a) (i) that are subject to Data Protection Laws of the European Union, the European Economic Area and/or their member states, Switzerland or any other applicable Data Protection Laws, and (ii) 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, (b) if and to the extent VTEX processes Personal Data for which such Affiliate(s) qualify as the Controller.

"**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 (i) the GDPR, (ii) any legislation in force from time to time in any Member State of the European Union or the European Economic Area, and Switzerland relating to privacy or the processing of personal data, including the Swiss Federal Data Protection Act 1992; (iii) any legislation in force from time to time in any other covered jurisdiction; and (iv) any guidance or statutory codes of practice issued or adopted by any Supervisory Authority or other applicable data protection authority or a Data Protection Board in relation to such legislations, in any case as applicable to the Processing of Personal Data under the Agreement and as updated, amended, replaced or superseded from time to time.

"**Data Subject**" means the identified or identifiable natural person to whom the Personal Data relates.

"**EU Restricted Transfer"** means a transfer of Contractor Data including Personal Data by Contractor or any Contractor Affiliate to VTEX or any VTEX Affiliate (or any onward transfer), in each case, where such transfer would be prohibited by European Data Protection Laws in the absence of the protection for the transferred Contractor Personal Data provided by the EU Standard Contractual Clauses.

"**EU Standard Contractual Clauses**" means the standard contractual clauses set out in the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the

European Parliament and of the Council, as amended or replaced from time to time by a competent authority under the relevant Data Protection Laws.

"**GDPR**" means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

"**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 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. For the purposes of this DPA, the Processor is VTEX.

"**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.

"**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 which is established by an EU Member State pursuant to Article 51 the GDPR and any similar regulatory authority responsible for the enforcement of Data Protection Laws.

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 Data Protection Laws.

Contractor shall have sole responsibility for the accuracy, quality, and lawfulness of Personal Data and the means by which Contractor acquired the Personal Data provided to VTEX. Contractor warrants that it has all necessary rights and needed consents, when required, 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.

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 Authorised Users;

(ii) Processing resulting from the use of the Services by Authorised 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 European Union or Member State law or 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 customised 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 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 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 their 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, as well as any other additional rights granted by the relevant Data Protection Laws to certain Data Subjects, as applicable (each, a "**Data Subject Request**"). Taking into account the nature of the Processing, VTEX shall assist Contractor by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment 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 instruction, 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 the provision of additional functionality(ies).

4. SUB-PROCESSORS

4.1. **Appointment of Sub-processors.** Contractor acknowledges and generally agrees that (a) VTEX's Affiliates may be retained as Sub-processors under this DPA 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 and in EU Standard Contractual Clauses (Module 3), to the extent applicable to the nature of the Services provided and the Personal Data processed 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 authorised 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 organisational measures for protection of the security, confidentiality and integrity of Personal Data in the context of the provision of the Services. VTEX's current measures are set forth in Appendix 2 to this DPA and may change from time to time to maintain compliance with this DPA and/or applicable Data Protection Laws. 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 2. 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 Services, but only to the extent required under 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 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. CONTRACTOR AFFILIATES

8.1. **Contractual Relationship**. The parties acknowledge and agree that, by executing the DPA, Contractor enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of the Contractor Affiliates, thereby establishing a separate DPA between VTEX and each such Contractor Affiliate subject to the provisions of the Agreement and Section 8 of this DPA. 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 the Contractor Affiliates. Each Contractor Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the avoidance of doubt, a Contractor 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 Contractor Affiliates must comply with the terms and conditions of the Agreement and this DPA and any violation of the terms and conditions of the Agreement and this DPA by a Contractor 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 the Agreement and this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Affiliates.

8.3. **Rights of Contractor Affiliates**. If a Contractor Affiliate becomes a party to the DPA with VTEX, it shall, to the extent required under 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 Data Protection Laws require the Contractor 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 Contractor 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 Contractor Affiliate individually but in a combined manner for all of its Contractor 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 Contractor 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 Contractor 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 Contractor 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 Contractor Affiliates, and, in particular, shall not be understood to apply individually and severally to Contractor and/or to any Contractor Affiliate that is a contractual party to any such DPA.

10. EUROPEAN SPECIFIC PROVISIONS

10.1. **Data Protection Laws**. VTEX Processes Personal Data in accordance with the Data Protection Laws to the extent directly applicable to VTEX's provisioning of the Services.

10.1.1. **Data Protection Impact Assessment**. Upon Contractor's request, VTEX shall provide Contractor with reasonable cooperation and assistance needed to fulfil Contractor's obligation under the Data Protection Laws to carry out a data protection impact assessment related to Contractor'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 and to the extent Contractor does not otherwise have access to the relevant information, and to such information is available to VTEX. VTEX shall provide reasonable assistance to the Contractor to consult the Supervisory Authority, prior to the Processing, to the extent required under the Data Protection Laws.

10.1.2. VTEX will notify the Contractor if it believes an instruction infringes the GDPR or other European Union or Member State Data Protection Laws.

10.1.3. **Restricted Transfers**. The Parties acknowledge that in providing the Services, VTEX will transfer Personal Data to recipients (including VTEX partners and Sub-processors) that may be located in countries outside the EEA. Such countries may not be deemed to offer an adequate level of data protection, as defined by the Data Protection Laws. Consequently, such transfers of Personal Data will be protected by appropriate safeguards mandated by the Data Protection Laws, including as the case may be the EU Standard Contractual Clauses or any additional safeguards as required by Data Protection Laws (each, a "**Restricted Transfer**").

In respect of any Restricted Transfer, the parties agree to the following:

10.1.3.1 In respect of any **EU Restricted Transfer**, Contractor and each Contractor Affiliate (each as "data exporter") and VTEX and each VTEX Affiliate (each as "data importer") with effect from the commencement of the relevant transfer hereby enter into the Module 2 – Controller to Processor of the EU Standard Contractual Clauses, the processing operations are deemed to be those described in Appendix 1 to this DPA. Appendix 2 to this DPA include the Technical and Organisational Measures applicable to the data transferred in the context of the processing activities carried out under this DPA.

10.1.3.2 The EU Standard Contractual Clauses made under clause 10.1.3.1 of this DPA come into effect on the later of:

- the Data Exporter becoming a Party to this DPA;

- the Data Importer becoming a Party to this DPA; and

- the commencement of the EU Restricted Transfer to which the EU Standard Contractual Clauses relate.

10.1.3.4 If, at any time, a Supervisory Authority or a court with competent jurisdiction over a party mandates that transfers from Controllers in the EEA to Processors established outside the EEA must be subject to specific additional safeguards (including but not limited to specific technical and organisational measures), the Parties shall work together in good faith to implement such safeguards and ensure that any transfer of Contractor Personal Data is conducted with the benefit of such additional safeguards.

10.1.4. **Onward transfers to Sub-processors.** The Parties acknowledge that, in providing the Services, VTEX will carry out Restricted Transfers to Sub-processors, in accordance with clause 10.1.3 of this DPA.

10.1.5. **Confidentially**. VTEX will ensure that persons authorised to Process Personal Data are subject to an appropriate contractual or statutory obligation of confidentiality.

11. 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.

12. GOVERNING LAW

As established in the Clause “Governing Law” in the Master Services Agreement.

13. 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 1B 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.

APPENDIX 1 - DESCRIPTION OF THE PROCESSING

1A. LIST OF PARTIES AND SUBPROCESSORS

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

The controller has authorised the use of the following processors and sub-processors:

1. **Controller to Processor**

    a. **Data exporter: VTEX CUSTOMER - IT MEANS THE CLIENT/CONTRACTING PARTY IDENTIFIED IN THE MASTER SERVICES AGREEMENT.**
    Role (controller/processor): Controller

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

    c. **Data importer: 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

    d. **Data importer (or exporter if Ireland applies): AWS**
    Name: Amazon Web Services Inc.
    Address: United States/work in progress to launch AWS storage in Ireland by 2023 depending on complexity of features
    Role (controller/processor): Subprocessor

1B. 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 specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Data Exporters may submit special categories of Personal Data to the Data Importer as the case may be, through the Services, the extent of which is determined and controlled by the Data Exporter 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 Proposal.

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. Please see Appendix 3.

COMPETENT SUPERVISORY AUTHORITY

Defined by the Contractor.

APPENDIX 2

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

The Data Importer has implemented and will maintain appropriate technical and organisational 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 organisational 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 materialisation, 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 GDPR, 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. There is work in progress to launch AWS storage in Ireland by 2023 depending on complexity of features. 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.

APPENDIX 3 – EU STANDARD CONTRACTUAL CLAUSES

CONTROLLER TO PROCESSOR (MODULE 2)

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Appendix 1 (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Appendix 1. (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Appendix 1

(d) The Appendix to these Clauses containing the Appendix referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b);

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Appendix 1.

Clause 7

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Appendix 1.

(b) Once it has completed the Appendix and signed Appendix 1, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Appendix 1.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Appendix 1. , unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Appendix 2 and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Appendix 1 After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter “personal data breach”). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Appendix 2. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is

not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Appendix 1.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefiting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of noncompliance. In

deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 15 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Appendix 2 the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its

sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Appendix 1, shall act as a competent supervisory authority.

(b) Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Appendix 1, shall act as competent supervisory authority.

(c) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practises affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practises in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practises that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practises of the third country of destination – including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practises not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or

organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law set out in the Master Services Agreement.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts defined in the Master Services Agreement.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

***