DATA PROCESSING AGREEMENT

Version Control:

Previous Version: 25th November 2025 available HERE.

Last Update: 23rd June 2026

INTRODUCTION

This Data Processing Agreement (“DPA”) is an addendum to and is incorporated into the Merchant Agreement ("Agreement") between the Merchant and Bamboo, referred to jointly as “Parties” or individually as “Party”, and applies to activities involving the Processing of Personal Data (as defined below) performed in connection with the Agreement and is an integral part of the Agreement for all legal purposes.

Any capitalized terms not otherwise defined in this DPA shall have the meaning given thereto in the DPA or the Applicable Laws. Except as modified below, the terms of the Agreement shall remain in full force and effect.

1. DEFINITIONS

1.1. In this DPA, the following terms shall have the meanings defined below:

1.1.1. "**Data Protection Requirements**" means, to the extent applicable: (i) European Data Protection Requirements; (ii) LATAM Data Protection Requirements;; (iii) mandatory industry rules and standards including, to the extent applicable, the Payment Card Industry Data Security Standard (“PCIDSS”); and (iv) any and all other Applicable Law related to data protection, data security, marketing, privacy, or the Processing of Personal Data.

1.1.2. "**Applicable Laws**" means any applicable law, regulation, directive, or other binding requirements (each as may be implemented, amended, extended, superseded, or re-enacted from time to time), including but not limited to, for the avoidance of doubt, Data Protection Requirements.

1.1.3. “**LATAM Data Protection Requirements**” means any and all Applicable Laws related to data protection, data security, marketing, privacy, or the Processing of Personal Data in the countries of South America, Central America, and Mexico, including but limited to:

- Brazil: Brazilian General Data Protection Law (Lei Geral de Proteção de Dados – LGPD);
- Panama: Panama Law No. 81 of 26 March 2019 on Personal Data Protection (Ley 81). and its implementing regulation, Executive Decree No. 285 of 28 May 2021;
- Mexico: Federal Law on Protection of Personal Data Held by Private Parties (LFPDPPP) (Ley Federal de Protección de Datos Personales en Posesión de los Particulares), published in 2010, together with its Regulations and Privacy Notice Guidelines.
- Colombia: Law 1581 of 2012 (General Data Protection Law), supplemented by Decree 1377 of 2013 and other regulatory provisions.
- Uruguay: Law No. 18,331 on Protection of Personal Data and Habeas Data Action (Ley de Protección de Datos Personales y Acción de Habeas Data), enacted in 2008, as amended.
- Chile: Law No. 19,628/1999 on Protection of Private Life (Ley sobre Protección de la Vida Privada) as amended by Lawy 21.719 effective from December 1st 2026.
- Peru: Personal Data Protection Law No. 29733 (Ley de Protección de Datos Personales), together with Supreme Decree No. 016-2024-JUS (Regulations).
- Argentina: Personal Data Protection Law No. 25,326 (Ley de Protección de los Datos Personales), enacted in 2000, with implementing regulations.

1.1.4. "**European Data Protection Requirements**" means any and all Applicable Laws related to data protection, data security, marketing, privacy, or the Processing of Personal Data in the European Union ("EU"), the European Economic Area ("EEA"), Switzerland, or United Kingdom ("UK"), including, to the extent applicable, the Regulation (EU) 2016/679 ("GDPR"), Directive 2002/58/EC, Directive 2009/136/EC, and UK GDPR, jointly with any local, amending or replacement legislation in any EU Member State or the UK. For the purposes of this DPA, "UK GDPR" means the GDPR as amended and incorporated into UK law under the UK European Union (Withdrawal) Act 2018.

1.1.5. "**Data Processing**" means any operation carried out with Personal Data, such as collection, production, receipt, classification, use, access, reproduction, transmission, distribution, processing, filing, storage, deletion, evaluation or control of the information, modification, communication, transfer, dissemination or extraction.

1.1.6. "**Merchant Data**" means any and all Personal Data that Bamboo Processes from or on behalf of the Merchant in connection with the Agreement, including information derived

from or combined with such Personal Data and the Personal Data of Merchant employees, contractors, and personnel, and Merchant Customers.

1.1.7. "**Bamboo Data**" mean all personal data from Bamboo's representatives processed by the Merchant to conduct its KYB processes.

1.1.8. "**Services**" means the services and other activities that will be provided or performed by Bamboo in accordance with the Agreement.

1.1.9. "**Data Processor**" means any natural or legal person who, on behalf of one of the Parties, processes Personal Data on behalf of the other Party under this DPA.

1.1.10. "**Agreement**" means the Merchant Agreement, including its addendums and annexes, containing the general terms for the provision of Services by Bamboo to the Merchant.

1.1.11. "**Jurisdiction-Specific Terms**" means all legal or regulatory terms, conditions, or rules that govern privacy and data protection and that apply within a particular geographic area or legal jurisdiction incorporated into this DPA.

1.1.12. "**Employee(s)**" means any employee, worker, including subcontractors or outsourced staff, representatives, or designees, remunerated or not, under a full or partial regime, who act on behalf of the Parties and have access to the Personal Data.

1.1.13. "**Government Authorities**" means any authority, including judicial, vested with powers to inspect, judge, and apply pertinent laws.

1.1.14. "**Security Incident**" means any adverse security event or set of events, confirmed or suspected, that impacts the availability, integrity, confidentiality, or authenticity of an information asset. In the case of this DPA, the expression will refer to incidents involving the Personal Data processed in the context of the Agreement.

1.1.15. "**End Date"** has the meaning described in this Agreement, where it is applicable.

2. JURISDICTION-SPECIFIC TERMS

2.1. Without limiting the foregoing, the Parties shall also comply with the following jurisdiction-specific terms to the extent such terms are applicable:

2.1.1. If LATAM Data Protection Requirements apply to the Data Processing or Personal Data shared by the Parties (as applicable) under the Agreement, then the terms available at Schedule A - LATAM Terms (incorporated into this DPA by this reference) shall apply to such data.

2.1.2. If European Data Protection Requirements apply to the Data Processing or Personal Data shared between Parties (as applicable) under the Agreement, then the terms available

at Schedule B - European Region Terms (incorporated into this DPA by this reference) shall apply to such data.

3. PROCESSING OF PERSONAL DATA

3.1. The performance of this Agreement requires the sharing of Personal Data between both Parties.

3.2. In relation to activities involving the Processing of Personal Data under the scope of the Agreement where each Party acts as sole Controller (i.e. when conducting KYB "**Know Your Business**" process to the other Party) , the Parties agree to:

3.2.1. Process the Personal Data in accordance with all Applicable Laws, including those coming into force after the signing of this DPA, ensuring in particular that every Data Processing activity be duly justified on one of the legal bases established by the Applicable Laws.

3.2.2. Process only the Personal Data necessary for executing the Agreement, including for the fulfillment of legal or regulatory obligations to which the Party is subject.

3.2.3. If the Party has access, in the context of the Contract, to Personal Data that it considers excessive or not necessary for the execution of the Contract, it shall immediately notify the other Party and disable such Personal Data.

3.2.4. If either Party performs any Data Processing activity unrelated to the performance of the Agreement, said Data Processing activity shall occur outside the context of this DPA. The Party that executes the Data Processing shall be deemed the sole Controller in relation to that activity, and the other Party shall be released from any obligation or liability derived therefrom.

3.2.5. Mutually cooperate to ensure proper compliance with the obligations relating to exercising the Data Subject's rights under the Applicable Laws applied and fulfilling any requests from the Government Authorities within the limit of their activities.

3.2.6. The Parties shall not use any type of tool, technology, reverse engineering, or other method intended to identify the Data Subjects, where Personal Data was shared in a manner that does not permit direct identification of the Data Subjects without cross-checking with other information or with access to the identification key.

3.2.7. The Parties shall not process, share, transfer, sell, rent, license, or otherwise make available any Personal Data to any third party for marketing, advertising, or promotional purposes.

3.3. In addition to the above, in relation to activities involving the Processing of Personal Data under the scope of the Agreement where Bamboo acts as a Processor and the Merchant acts as Controller, Bamboo also agrees to:

3.3.1. Use the Merchant's Data solely for the purposes inherent to the Agreement and, under no circumstances, for purposes other than those. Bamboo shall not be held liable for any loss or damage, or for any claim (including, but not limited to, claims or complaints filed by a data subject or a regulator) arising from any action or omission by Bamboo, insofar as such action or omission results from the Merchant's instructions or is based on inaccurate, incorrect, or incomplete data or information provided by the Merchant.

3.3.2. Process Merchant's Data in accordance with the Merchant's instructions. If Bamboo considers that any of the instructions infringe any provision regarding personal data protection, Bamoo shall immediately inform the Merchant.

3.3.3. Maintain, in writing, a record of all categories of processing activities carried out on behalf of the Merchant.

3.3.4. Maintain the duty of confidentiality regarding personal data accessed in the course of providing the Services, even after their completion.

4. PARTIES EMPLOYEES

4.1. The Parties shall ensure that the Data Processing of Personal Data performed in the context of the Agreement will be restricted to the Employees responsible for the Data Processing and exclusively to the extent necessary to execute the Agreement.

4.2. The Parties Employees must

a. receive training regarding Data Protection principles and Data Protection Requirements.
b. know the Parties' obligations, including those contemplated in this Agreement.
c. be subject to confidentiality agreements or professional or statutory confidentiality and data protection obligations.

5. SECURITY REQUIREMENTS

5.1. Each Party shall implement appropriate technical, administrative, and organizational measures compatible with the Data Processing activities performed. To assess the appropriate level of security, the Parties shall consider the risks posed by the Data Processing activity, particularly those related to Security Incidents.

5.2. The Parties information security and privacy program must at least:

a. Protect against the unauthorized or unlawful Processing of Personal Data.
b. Meets the applicable standards of industry practice relevant to its activities and the volume and sensitivity of the Personal Data, including the appropriate physical, technical, and organizational measures that protect against unauthorized or unlawful Data Processing.
c. Includes an appropriate network security program.
d. Complies with Data Protection Requirements applicable to the Processing thereof.

5.3. The Parties must undertake regular testing, assessing, and evaluation of the effectiveness of the technical, administrative, and organizational measures for ensuring the security of operations involving the Processing of Personal Data.

6. SUBCONTRACTORS

6.1. Each Party provides the other Party with a general authorisation to the Party to disclose Personal Data to financial institutions, partners, and suppliers necessary for the proper execution of the Agreement; to auditing firms for any required reviews in financial, accounting, anti–money laundering, and related matters; to electronic signature entities for signature management; and to regulatory bodies in cases legally established. Likewise, personal data may be processed by other entities within the BAMBOO Group for internal administrative purposes and for the proper execution of the Agreement, as well as by authorized international providers, under conditions of security and confidentiality, in accordance with the corresponding legal safeguards, information about which may be obtained by email at dpo@bamboopayments.com.

6.2. When any Data Processing activity is carried out through a Subcontractor, the Parties must, in relation to this Subcontractor:

6.2.1. Preserve the integrity and accuracy of the Personal Data and must update, correct, or delete such Personal Data at the request of the other Party, when required by Applicable Laws or by the Data Subject (when applicable);

6.2.2. Verify, through due diligence or equivalent procedure, that each Subcontractor is able to guarantee a level of Personal Data protection, at least equivalent to this DPA and provide evidence of this verification;

6.2.3. Enter into a formal agreement with each Subcontractor, ensuring that the agreement includes provisions at least equivalent to those in this DPA; and

6.2.4. Be exclusively liable for any and all actions and omissions related to the Data Processing conducted by any of its Subcontractors.

7. INTERNATIONAL DATA TRANSFERS

7.1. If an international data transfer by either Party is necessary for the performance of the Agreement, and the country of destination has not been considered adequate by the Government Authority of the country where the exporting Party is located, then the exporting Party shall ensure that the international data transfer will be made pursuant to one of the mechanisms contemplated in the Applicable Laws.

8. DATA SUBJECTS RIGHTS

8.1. The Parties shall mutually cooperate in complying with the obligations related to exercising Data Subjects' rights per Applicable Laws.

8.2. The Parties shall:

8.2.1. Immediately notify the other Party upon receiving a request from the Data Subject when related to any Data Processing activity performed under the Agreement;

8.2.2. Refrain from responding to any Data Subject's request related to the Personal Data of the other Party until that Party provides written consent to the contents of the response, except where the Applicable Laws require a response within less than 48 (forty-eight) hours; and

8.2.3. If the informed Party does not provide the written consent until 2 (two) business days before the end of the timeframe required by the Applicable Laws, the other Party is allowed to fulfill the Data Subject's request.

9. SECURITY INCIDENT

9.1. When a Party identifies the occurrence of a Security Incident that may (i) cause risk or relevant damage to Data Subjects under the Applicable Laws; and (ii) impact the object of the Agreement, such Party shall immediately notify the other Party.

9.2. The notice shall include sufficient information for the affected Party to comply with any requirements imposed by Applicable Laws, including but not limited to: (i) the description of the nature of the Personal Data and the Data Subjects involved; (ii) the technical and security measures adopted to protect such Personal Data; (iii) the measures taken (and those in the process of being taken) to mitigate the effects of such Security Incident; (iv) the risks related

to such Security Incident; and (v) any additional information that may help facilitate the understanding of the Security Incident, its causes and consequences, and/or that may be required by the Government Authorities.

9.3. The Parties shall investigate the causes and consequences of the Security Incident at their own expense and take the necessary measures to remedy its consequences, promptly informing the other Party about all measures taken.

9.4. The Parties shall maintain records on the Security Incident, including at least (a) a description of the nature of the Security Incident, (b) a description of the consequences of the Security Incident, and (c) a description of the measures taken or proposed by the other Party to cope with the Security Incident.

9.5. Where the Security Incident involves both Parties, the Parties shall not disclose any information concerning the Security Incident unless otherwise authorized in by the other Party or required by the Government Authorities' determination, pursuant to the Applicable Laws.

10. GOVERNMENT AUTHORITIES

10.1. The Parties shall mutually cooperate in complying with obligations or requests imposed by any competent Government Authority.

10.2. The Parties shall immediately inform the other Party upon receiving requests for information or determinations from the Government Authorities relating to any Data Processing activity performed within the context of the Agreement, except when the request is under a gag order or any other type of legal restriction that prevents the communication to be made. If such requests or determinations are related to the Personal Data shared by the other Party, then the Party subpoenaed shall submit a suggestion of answer for the other Party's validation within the time period prescribed by law or determined by the Government Authorities.

11. EXCLUSION AND RETURN OF PERSONAL DATA

11.1. Upon completion of the activities involving the Data Processing of Personal Data under the Agreement, each Party shall cease to process the other Party’s Personal Data and, upon written request, return or delete the Personal Data related to the completed activities, along with all existing copies (in digital or physical form), unless retaining the data is necessary to comply with Applicable Laws (especially in contractual, tax, and accounting matters).

12. INDEMNIFICATION AND LIABILITY

12.1. The Parties acknowledge that all indemnification and liability obligations are governed solely by the Agreement. Nothing in this DPA shall be construed to create, expand, or modify any indemnification or liability obligations beyond those expressly provided in the Agreement.

12.2. The Parties shall comply with all Applicable Laws and this DPA in the performance of their respective obligations. Any liability arising solely from noncompliance with this DPA shall be subject to the limits and terms of liability set forth in the Merchant Agreement.

12.3. This DPA does not create joint liability between the Parties. Each Party shall remain severally liable only to the extent provided in the Merchant Agreement.

12.4. Any reference in this DPA to indemnification or liability is for the purpose of interpreting the obligations under the Merchant Agreement and shall not be deemed to create additional obligations beyond those in the Merchant Agreement.

13. GENERAL PROVISIONS

13.1. Without prejudice to any provisions regarding mediation and jurisdiction:

13.1.1. The Parties hereto submit to the choice of the jurisdiction stipulated in the Agreement in connection with any disputes or claims that may in any way result from this DPA, including disputes relating to its existence, validity, or termination or the consequences of its nullity, and

13.1.2. This DPA and all extracontractual or other obligations arising out of or relating to this DPA shall be governed by the laws of the country or territory stipulated for this purpose in the Agreement.

13.2. In the event of a conflict between the provisions of this DPA and the Agreement or any other document performed between the parties, specifically in connection with activities involving the Data Processing of Personal Data, the provisions of this DPA shall prevail, except where a supervening document is executed between the Parties, expressly declaring the subsidiary nature of this DPA.

13.3. This DPA may be amended at the Parties' discretion or in the event of a supervising law, regulation, or determination by the Government Authority requiring a change in its provisions. The new provisions shall be agreed upon in good faith by the Parties and always in writing as an amendment to this DPA.

13.4. If any provision of this DPA is held void, invalid, or unenforceable, the remaining provisions shall remain in full force and effect. The void, invalid, or unenforceable provision shall be amended to ensure its validity and effectiveness while preserving the Parties' intention.

13.5. This DPA shall remain in effect until termination of the Agreement for any reason.

13.6. This DPA shall survive the expiration of the Agreement and continue to bind the Parties in relation to activities involving the Data Processing of Personal Data which originate from the Agreement and continue to be performed, though only for purposes of complying with a legal or regulatory obligation.

13.7. This DPA is performed and becomes an integral and mandatory part of the Agreement, with effects as of the date hereof. It applies, however, to all activities regarding the Data Processing of Personal Data performed since the date of performance of the Agreement.

SCHEDULE A: LATAM TERMS

1. **DEFINITIONS**: In addition to the defined terms in the DPA, the following definitions apply to the LATAM Terms:
   1.1. “controller”, “data subject" and “data protection authority” and their variations shall have the same meanings as in the applicable LATAM Data Protection Requirements.
   1.2. "ANPD" means the Brazilian National Data Protection Authority.

2. **PROCESSING TERMS**:
   2.1. The execution of the Agreement encompasses the mutual sharing of Personal Data according to the scope of the Agreement.
   2.2. Each Party will act as sole Controller in relation to the processing of Personal Data for the purpose of conducting KYB or KYC process (“**Know Your Business**” or “**Know Your Customer**”). However, if Bamboo processes the Merchant’s Data for the purpose of providing its payment processing services it will act as Data Processor on behalf of the Merchant and the Merchant as Controller. In both cases, where the Parties are subject to the LATAM Data Protection Requirements, the Parties agree as follows:
      2.2.1. Each Party shall be individually responsible for ensuring that its Processing of the Personal Data is lawful, fair, and transparent following LATAM Data Protection Requirements, including where applicable on the basis that the data subject has unambiguously given his or her explicit consent, or on the basis of some other valid ground provided for in LATAM Data Protection Requirements.
      2.2.2. When Bamboo acts as Data Processor and the Merchant acts as Controller:
         a. When consent is the basis of Data Processing, the Merchant shall be responsible for obtaining the express, free, unambiguous, and informed consent of the data subject, according to the LATAM Data Protection Requirements.
         b. Bamboo will appropriately assist the Merchant in the event of a Security Incident, a notice, inquiry, audit, or investigation by the ANPD or any other relevant regulator, or of a complaint, inquiry, or request received directly from a data subject, or any third party audit, that relates to the Processing of Personal Data pursuant to the Agreement, by providing information about the relevant Processing as required for the Merchant to fulfill its obligations under the LATAM Data Protection Requirements.

c. Bamboo shall only process Personal Data as clearly instructed by the Merchant or in accordance with the terms of the Agreement or as permitted by Applicable Law.

3. **INTERNATIONAL TRANSFERS:** To the extent that any Party Processes or otherwise transfers Merchant Data or Personal Data (as applicable) outside the jurisdiction in which such data was originally collected or otherwise Processed by, or on behalf of, the Merchant:

3.1. Each Party shall be responsible for complying with any requirement for authorization or registration of transfer outside of the country of origin in accordance with LATAM Data Protection Requirements.

3.2. Such transfer shall be subject to any conditions that may be reasonably imposed by the other Party, including that each Party (or any relevant Subcontractor) enters into (and complies with) any data transfer agreement reasonably acceptable to the other Party and consistent with LATAM Data Protection Requirements.

3.3. When the Data Subjects are located in Argentina, Colombia, Uruguay, Panama, Mexico, Chile, and Peru and such jurisdiction of destination is not considered adequate under the transferor's local data protection law, the Model Contractual Clauses of Red Iberoamericana de Protección De Datos (https://www.redipd.org/en/document/annex-model-contractual-clausesen.pdf) shall apply:

a. **ANNEX A**: Accession Forms for New Partners.

Not applicable.

b. **ANNEX B**: Description of the Transfer

- If Bamboo acts as a Data Processor and Merchant as Controller:
  - Categories of Data Subjects whose Personal Data is transferred:

    Merchant's customers or users.
  - Sensitive Personal Data transferred (if applicable) and restrictions or safeguards applied: no-applicable.
  - Transfer Frequency: Ongoing
  - Term: in Accordance with Applicable Laws to comply with contractual, tax, anti-money laundering obligations.
  - Purpose(s) of the data transfer and further processing: payment processing, fraud prevention (if applicable), and identity verification.
  - Subcontractors: Merchant's data may be disclosed to financial institutions, partners, and suppliers necessary for Bamboo to provide the payment

processing services; to auditing firms for any required reviews in financial, accounting, anti–money laundering, and related matters; to electronic signature entities for signature management; and to regulatory bodies in cases legally established. Likewise, Merchant's Data may be processed by other entities within the BAMBOO Group for internal administrative purposes and for the proper execution of the Service.

- When each Party acts as a Controller:
  - Categories of Data Subjects whose Personal Data is transferred: each Parties' representatives.
  - Sensitive Personal Data transferred (if applicable) and restrictions or safeguards applied: no-applicable.
  - Transfer Frequency: Upon KYB/KYC process.
  - Term: in accordance with Applicable Laws to comply with contractual, tax, anti-money laundering obligations.
  - Purpose(s) of the data transfer and further processing: AML and identity verification.
  - Subcontractors: Personal Data may be disclosed to financial institutions, partners, and suppliers necessary for each party to comply with its compliance obligations; to auditing firms for any required reviews in financial, accounting, anti–money laundering, and related matters; to electronic signature entities for signature management; and to regulatory bodies in cases legally established.

    Likewise, Personal Data may be processed by other entities within the BAMBOO Group for internal administrative purposes and for the proper execution of the Service.

c. **ANNEX C**: Administrative, Physical, and Technical Measures to Ensure Data Security: According to the Information Security Policy and PCI-DSS controls.

3.5. When the Data Subjects are located in Brazil and there is not an adequacy decision issued by the ANPD on the jurisdiction or international organization where personal data is transferred to, the Standard Contractual Clauses, Resolução CD/ANPD nº 19/2024 (https://www.gov.br/anpd/pt-br/acesso-ainformacao/institucional/atos-

normativos/regulamentacoes_anpd/regulationon-international-transfer-of-personal-data.pdf , of ANPD shall apply:

a. **CLAUSE 1: Identification of the Parties.**

As identified in the Agreement.

b. **CLAUSE 2: D**

- When each party acts as Data Controller:
  - Data Exporter: Party whose Personal Data is requested.
  - Data Importer: Party requesting KYB process.
  - Purpose of processing: KYB process.
  - Category of personal data transferred: identification Personal Data (name, date or birth, nationality, address, phone, email address, IP address and device identifier, government identification number(. Additional data may be transferred according to regulations and the Parties Privacy Notice.
  - Period of data storage: according to clause 11 of this DPA.
- When Bamboo acts as Data Processor:
  - Data Exporter: Merchant and its Affiliates , as defined in the Agreement.
  - Data Importer: Bamboo and its Affiliates, as defined in the Agreement.
  - Purpose of processing: payment processing.
  - Category of personal data transferred: identification Personal Data (name, phone, date or birth, nationality, address, email address, IP address and device identifier, government identification number), purchase information. Additional data may be transferred according to regulations and the Parties Privacy Notice.
  - Period of data storage: according to clause 11 of this DPA.

c. **CLAUSE 3:** Option B

Third Party Recipients:

- financial institutions (banks, payment facilitators or any type of payment processor that partners with Bamboo).
- auditing, accounting and legal firms.
- fraud prevention and AML SaaS.
- electronic signature SaaS.
- cloud service Providers.
- payment processors.

- customer support tools.
- hosting providers.
- security providers services.
- other entities within the BAMBOO Group.

d. CLAUSE 4: Option A

Responsible for publishing the document requested in Clause 14: Exporter and Importer.

Responsible for responding to requests from holders referred to in Clause 15: Exporter and Importer.

Responsible for carrying out the security incident communication provided for in Clause 16: Exporter and Importer.

3.4. The Parties shall cooperate in carrying out any assessment of such transfer required under LATAM Data Protection Requirements.

SCHEDULE B: EUROPEAN REGION TERMS

1. **DEFINITIONS:** In addition to the defined terms in the DPA, the following definitions apply to these European Region Terms:
   1.1. The terms “controller”, “data subject”, “Data Processor”, and “supervisory authority” shall have the same meanings as in the GDPR or the UK GDPR (as applicable), and the terms “processed” and “process” shall be construed in accordance with the definition of “processing” described below. The terms “personal data” and “processing” in these European Region Terms shall have the same meanings as in the GDPR or the UK GDPR (as applicable) and not, for the avoidance of doubt, the definitions of “Personal Data” and “Processing” as set out in the DPA.
   1.2. “Approved Purpose” means the purpose(s) for which Bamboo may process the personal data it receives from the Merchant as a Data Processor following the Agreement including conducting the process of Know Your Customer, as may be expressly specified in the Agreement.
   1.3. "Controller" means the Merchant who acts as controller of personal data subject to the GDPR or UK GDPR and processed in connection with the Agreement or in the performance of the Services, as well as Bamboo and its Affiliates who act as a controller to conduct KYB process to the Merchant.
   1.4. "SCCs" means the European Commission’s standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 as set out in annex to Commission Decision 2021/914, which, as of the Last Updated date, are available at https://eur-lex.europa.eu/legalcontent/EN/TXT/HTML/?uri=CELEX:32021D0914, and which are incorporated herein by reference.
   1.5. "UK Addendum" means the UK Information Commissioner's Office's International Data Transfer Addendum to the SCCs, which, as of the Last Updated date, is available at https://ico.org.uk/media/fororganisations/documents/4019483/international-data-transfer-addendum.pdf, and which is incorporated herein by reference.

2. PROCESSING TERMS

2.1. For the purpose of payment processing in accordance with the scope of the Agreement, Bamboo will act as a Data Processor and the Merchant as sole Controller. However, each Party acts as sole Controller when conducting KYB to the other Party. In each case, where the Parties are subject to the European Data Protection Requirements, the Parties agree as follows:

2.2. If personal data is exchanged between the Parties in connection with the Agreement or the provision of the Services for the purpose of conducting KYB to the other Party:

a. To the fullest extent permitted by applicable European Data Protection Requirements, the Parties shall each be independent controllers of the personal data and, as such shall independently determine the purposes and the means of the processing of that personal data;

b. Each Party shall be individually responsible for ensuring that its processing of the personal data is lawful, fair, and transparent in accordance with applicable European Data Protection Requirements, including where applicable on the basis that the data subject has unambiguously given his or her consent, or on the basis of some other valid ground provided for in applicable European Data Protection Requirements; and

c. Each Party shall implement and maintain appropriate technical and organisational measures to protect any such personal data in their possession or control from: (i) accidental or unlawful destruction; and (ii) loss, alteration, or unauthorised disclosure or access, and which provide a level of security appropriate to the risk represented by any processing and the nature of the personal data to be protected.

2.3 If personal data is exchanged between the Merchant and Bamboo in connection with the Agreement or the provision of the Services for the purpose of processing payments:

a. The Merchant shall act as the Controller of the personal data and shall determine the purposes and means of the processing of such personal data. Bamboo shall act solely as a Data Processor on behalf of the Merchant and shall process the personal data only in accordance with the Merchant's documented instructions, unless otherwise required by applicable law.

b. The Merchant shall be responsible for ensuring that its processing of the personal data is lawful, fair, and transparent in accordance with applicable European Data Protection Requirements, including where applicable on the basis that the data subject has unambiguously given his or her consent, or on the basis of some other valid legal ground provided for in applicable European Data Protection Requirements.

c. Bamboo, as Data Processor, shall implement and maintain appropriate technical and organizational measures to protect any personal data in its possession or control from: (i) accidental or unlawful destruction; and (ii) loss, alteration, or unauthorized disclosure or access, providing a level of security appropriate to the risk represented by the processing and the nature of the personal data to be protected.

d. Bamboo shall process the personal data only for the purpose of performing the Services under the Agreement and in accordance with the Merchant's instructions, and shall not use the personal data for any other purpose.

3. INTERNATIONAL TRANSFERS

3.1. If personal data of people located in the European Economic Area or UK is transferred to a country or territory which is, at the time of such transfer, is not deemed to ensure an adequate level of protection by the European Commission or by the UK Information Commissioner's Office, then such transfer shall be governed by the SCCs, incorporated to this Addendum (https://eurlex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914).

3.2. For the purposes of the EU SCCs, the following shall apply:

a. If Bamboo acts as a Data Processor, Module Two (Controller to Processor) shall apply.

- Clause 9: Option 2: General Written Authorization.
- Clause 17: as defined in the Agreement.
- Clause 18: The EU Member State where any dispute arising from these Clauses shall be resolved is the courts of the jurisdiction stipulated in the Agreement.

b. If Bamboo acts as a Controller, Module One (Controller to Controller) shall apply.

- Clause 9: Option 2: General Written Authorization.
- Clause 17: as defined in the Agreement.
- Clause 18: The EU Member State where any dispute arising from these Clauses shall be resolved is the courts of the jurisdiction stipulated in the Agreement.

3.3. For the purposes of the Annex I of the SCCs:

3.4. Annex I: LIST OF THE PARTIES

3.4.1. If Bamboo acts as a Data Processor and Merchant as a Controller:

- Data exporter(s):
  - Name: Merchant and its Affiliates, as defined in the Agreement.
  - Address: as defined in the Agreement.

- Contact person's name: as defined in the Agreement.
- Activities relevant to the data transferred under these Clauses: All data processing activities agreed under the Agreement.
- Signature and date: Signed and dated for and on behalf of the data exporter by execution of the Agreement.
- Role: Controller.

- Data importer(s):
  - Name: Bamboo and its Affiliates, as defined in the Agreement.
  - Address: as defined in the Agreement.
  - Contact person's name: Luz Elena Arambarri, Data Protection Officer, dpo@bamboopayment.com
  - Activities relevant to the data transferred under these Clauses: All data processing activities agreed under the Agreement.
  - Role: Data Processor.
  - Signature and date: Signed and dated for and on behalf of the data importer by execution of the Agreement.
- Description of Transfer
  - Categories of data subjects whose personal data is transferred: Merchant's customers.
  - Categories of personal data transferred: identification personal data (name, phone, email address, address, date of birth, IP address and device identifier, government identification number, purchase information). Additional data may be transferred according to regulations.
  - Sensitive data transferred: not applicable.
  - The frequency of the transfer: the data transfer is continuous throughout the provision of the services.
  - Nature and purpose of the processing: Bamboo's activity is as described in the Services under the Agreement. These responsibilities are focused on facilitating the Merchant's payment processing. This includes receiving payment information from the Merchant's customers, verifying its accuracy and completeness, obtaining payment authorization, and settling the authorized funds directly with the Merchants.

- The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: Bamboo shall process Personal Data during the term of the Agreement and the required by the Applicable Law and not thereafter, except if the Merchant explicitly instructs Bamboo to do so.

- Supervisory Authority: In accordance with Clause 13: as defined in the Agreement.

3.4.2. If each Party acts as a Controller:

- Data exporter(s):
  - Name: Each Party and its Affiliates, as defined in the Agreement.
  - Address: as defined in the Agreement.
  - Contact person's name: as defined in the Agreement.
  - Activities relevant to the data transferred under these Clauses: All data processing activities agreed under the Agreement.
  - Signature and date: Signed and dated for and on behalf of the data exporter by execution of the Agreement.
  - Role: Controller.
- Data importer(s):
  - Name: Each Party and its Affiliates, as defined in the Agreement.
  - Address: as defined in the Agreement.
  - Contact person's name: From Bamboo Luz Elena Arambarri, Data Protection Officer, dpo@bamboopayment.com
  - Activities relevant to the data transferred under these Clauses: All data processing activities agreed under the Agreement.
  - Role: Controller
  - Signature and date: Signed and dated for and on behalf of the data importer by execution of the Agreement.
- Description of Transfer
  - Categories of data subjects whose personal data is transferred:
    Each Party's representatives.
  - Categories of personal data transferred: identification personal data (name, phone, email address, address, role, government identification number, date

of birth, nationality. Additional data may be transferred according to regulations and the Parties Privacy Notice.

- Sensitive data transferred: not applicable.
- The frequency of the transfer: Every time KYB needs to be conducted according to each Party's policies.
- Nature and purpose of the processing: To conduct KYB process in accordance with Applicable Law.
- The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: Each Party shall process Personal Data during the term of the Agreement and the required by the Applicable Law and not thereafter, except if the other Party explicitly instructs Bamboo to do so.

- Supervisory Authority: In accordance with Clause 13: as defined in the Agreement.

3.5. Without prejudice to the provisions set out in Sections 4.2 to 4.6 of these European Region Terms, nothing in the Agreement or this DPA (including these European Region Terms) is intended to vary or modify the SCCs. The Merchant and Bamboo agree that the optional Section I, Clause 7, and the optional paragraph in Section II, Clause 11 in the SCCs shall not apply.

3.6. For the purposes of the UK Addendum, as permitted by Clause 17 of such addendum, the parties agree to change the format of the information set out in Part 1 of the addendum so that:

- the details of the parties in Table 1 shall be as set out above (with no requirement for signature);
- for the purposes of Table 2, the addendum shall be appended to the EU SCCs (including the selection of modules and the application/disapplication of such optional clauses as specified above); and
- the appendix information listed in Table 3 is as set out above.

3.7. In the event that the SCCs or the UK Addendum are (i) deemed invalid by the European Commission, the UK Information Commissioner's Office, a relevant regulator, or supervisory authority for whatever reason, or (ii) superseded by other standard contractual clauses issued or approved by the European Commission, the UK Information Commissioner's Office, a relevant regulator or supervisory authority, the Merchant and Bamboo shall immediately

comply with such other standard contractual clauses or any other valid mechanism under European Data Protection Requirements for transferring and processing personal data outside the EEA and/or the UK (as applicable).

3.8. Annex II. Technical and organisational measures: In accordance with Bamboo's Information Security Policy, PCI-DSS controls.