

DATA PROCESSING AGREEMENT

This Data Processing Agreement (“**DPA**”) is subject to and forms part of the Platform Services Agreement (“**PSA**”) and governs MontyPay’s and its Affiliates’ Processing of Personal Data.

1. DEFINITIONS

In addition to the definitions set out in the PSA, capitalized words and phrases used in this DPA shall have the following meanings:

“**Data Controller**” means the entity which alone or jointly with others determines the purposes and the means of the Processing of Personal Data.

“**Data Processor**” means the entity which Processes Personal Data on behalf of a Data Controller.

“**Data Subject**” means Customer, employee of Merchant, employee of MontyPay, or other natural person whose Personal Data are processed in the context of this Agreement.

“**Data Protection Law**” means the EU General Data Protection Regulation 2016/679 (as amended and replaced from time to time) and the e-Privacy Directive 2002/58/EC (as amended by Directive 2009/136/EC, and as amended and replaced from time to time) and their national implementing legislations; the UK Data Protection Act (as amended and replaced from time to time); and the Data Protection Acts of the European Economic Area (“EEA”) countries (as amended and replaced from time to time).

“**GDPR**” means the General Data Protection Regulation (EU) 2016/679.

“**Processing of Personal Data**” means to perform any operation or set of operations on Personal Data or sets of Personal Data, such as collecting, recording, organizing, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing by transmission, disseminating or otherwise making available, aligning or combining, restricting, erasing or destroying, as described under Data Protection Law.

“**Personal Data**” means any information relating to an identified or identifiable natural person that is Processed in connection with the Services and includes “personal data” as defined under the GDPR.

“**Sub-Processor**” means the entity engaged by the Data Processor or any further sub-contractor to Process Personal Data on behalf of and under the instructions of the Data Controller.

2. ROLES OF THE PARTIES

2.1 Where MontyPay processes Personal Data while performing the Services MontyPay will act as a Data Processor for the Merchant, other than in the circumstances where MontyPay determines the purpose and the manner of Processing of Personal Data and subsequently act as a Data Controller, as described in clause 2.2 below.

2.2 Merchant authorizes MontyPay to Process Personal Data, as a Data Controller, in the following cases:

(a) Where MontyPay determines the purpose and the manner of Processing of Personal Data, for example, in order to: (i) comply with the Applicable Law (including specifically anti-money laundering and counter-terrorism financing laws and regulations), Payment Scheme Rules, Data Protection Law, GDPR, or (ii) perform any obligation under the PSA;

(b) Where MontyPay Processes Personal Data for the purpose of internal research, fraud, security and risk management and assessing financial, credit, or information security risk.

3. OBLIGATIONS OF MERCHANT

3.1 The Merchant represents and warrants to MontyPay that, in relation to the Processing of Personal Data in the context of the Services, it acts as a Data Controller and that it:

3.1.1 Complies with Data Protection Law and MontyPay’s Privacy Policy in respect of Processing of Personal Data, and only gives lawful instructions to MontyPay. The Merchant must comply with the personal data protection laws of the countries in which the Merchant provides its services and operates, in particular when Processing and sending the Personal Data to MontyPay in the context of using the Services and submitting Transactions.

3.1.2 Relies on a valid legal ground under Data Protection Law for each purpose of its personal data processing activities, including obtaining Data Subjects’ appropriate consent if required or appropriate under Data Protection Law.

3.1.3 Provides appropriate notice to the Data Subjects regarding: (a) the Processing of Personal Data for the purpose of providing the Services, in a timely manner and at the minimum with the elements required under Data Protection Law; (b) the existence of Data Processors located outside of Europe.

3.1.4 Takes reasonable steps to ensure that Personal Data is accurate, complete and current; adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed; and kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are processed unless a longer retention is required or allowed under Applicable Law.

3.1.5 Implements appropriate technical and organizational measures to ensure, and to be able to demonstrate, that the Processing of Personal Data is performed in accordance with Data Protection Law, including, as appropriate, appointing a data protection officer, maintaining records of processing, complying with the principles of data protection by design and by default and, where

required, performing data protection impact assessments and conducting prior consultations with supervisory authorities.

3.1.6 Responds to Data Subject requests to exercise their rights of: (i) access; (ii) rectification; (iii) erasure; (iv) data portability; (v) restriction of Processing of Personal Data; and (vi) objection to the Processing of Personal Data in accordance with Data Protection Law.

3.1.7 Cooperates with MontyPay to fulfil their respective data protection compliance obligations in accordance with Data Protection Law.

3.1.8 Ensures that all Merchant staff are appropriately trained in line with their responsibilities under Data Protection Law.

3.1.9 With respect to Processing of Personal Data as described in article 22 of the GDPR, should such processing occur, it has put in place suitable measures to safeguard the Data Subject's rights and freedoms and legitimate interests and the right to obtain human intervention on the part of the Merchant, to allow Data Subjects to express their point of view and to contest the decision made in relation to the Data Subject.

4. OBLIGATIONS OF MONTYPAY

MontyPay will:

4.1 Only Process Personal Data in accordance with the Merchant's lawful written instructions and not for any other purposes than as required for: (i) the provision of the Services by MontyPay; (ii) MontyPay's role as a Data Controller as described in clause 2.2; or (iii) other purposes agreed by both Parties in writing.

4.2 Promptly inform Merchant if, in its opinion, the Merchant's instructions infringe Data Protection Law, or if MontyPay is unable to comply with the Merchants' instructions.

4.3 Cooperate with the Merchant in its role as Data Controller to fulfil its own data protection compliance obligations under Data Protection Law, including by providing all information available to MontyPay as necessary to demonstrate compliance with the Merchant's own obligations and where applicable to help Merchant conducting data protection impact assessments or prior consultation with supervisory authorities.

4.4 Keep internal records of Processing of Personal Data carried out as a Data Processor on behalf of Merchant.

4.5 Assist Merchant in fulfilling its obligation to respond to Data Subjects' requests to exercise their rights as provided under Data Protection Law and notify Merchant about such requests if MontyPay receives it directly from the Data Subject.

4.6 Notify Merchant when local laws prevent MontyPay from: (a) fulfilling its obligations under this Agreement and have a substantial adverse effect on the guarantees provided by this Agreement; and

(b) complying with the instructions received from the Merchant via this Agreement, except if such disclosure is prohibited by Applicable Law, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation.

4.7 When the Agreement expires or upon termination of the Agreement or upon a request to delete or return Personal Data by Merchant, except for any Personal Data which MontyPay processes as a Data Controller, MontyPay will, at the choice of Merchant, delete, anonymize, or return such Personal Data to Merchant, and delete or anonymize existing copies unless applicable law prevents it from returning or destroying all or part of the Personal Data or requires storage of the Personal Data (in which case MontyPay will protect the confidentiality of the Personal Data and will not actively Process the Personal Data anymore).

5. DATA TRANSFERS

5.1 Merchant authorizes (and confirms that it has obtained, on behalf of MontyPay, the required informed consents from the Customers and Merchant's employees, directors and shareholders) MontyPay to transfer the Personal Data Processed in connection with the Services outside of the EEA and UK in accordance with lawful data transfer mechanisms that provide an adequate level of protection under Data Protection Law and appropriate or suitable safeguards as required by Applicable Law.

6. SUB-PROCESSING

6.1 Merchant gives general authorization to MontyPay to Process and sub-process Personal Data using internal and external Sub-Processors in the context of the Services under the conditions set forth below and MontyPay represents and warrants that when sub-processing the Processing of Personal Data in the context of the Services, it:

- (a) Binds its internal Sub-Processors to respect the Standard Contractual Clauses and to comply with the Merchant's instructions.
- (b) Requires its external Sub-Processors, via a written agreement, to comply with the requirements of Data Protection Law applicable to processors and data transfers, with the Merchant's instructions and with the same obligations as are imposed on MontyPay by this Agreement. This will be done by using the Standard Contractual Clauses or another appropriate transfer solution.
- (c) Remains liable to the Merchant for the performance of its Sub-Processors' obligations.
- (d) Will inform Merchant of any addition or replacement of a Sub-Processor in a timely fashion so as to give Merchant an opportunity to object to the change or to terminate the Agreement before the Personal Data is communicated to the new Sub-Processor, except where the Services cannot be provided without the involvement of a specific Sub-Processor.

7. SECURITY; CONFIDENTIALITY; PERSONAL DATA BREACH

7.1 The Parties must implement and maintain a comprehensive written information security program with appropriate technical and organizational measures to ensure a level of security appropriate to

the risk, which includes, as appropriate: (a) the pseudonymization and encryption of Personal Data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing. In assessing the appropriate level of security, the Parties must take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing of Personal Data as well as the risk of varying likelihood and severity for the rights and freedoms of Data Subjects and the risks that are presented by the Processing of Personal Data, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise Processed.

7.2 The Parties must take steps to ensure that any person acting under their authority who has access to Personal Data is subject to a duly enforceable contractual or statutory confidentiality obligation, and if applicable Process Personal Data in accordance with the Controller's instructions.

7.3 The Parties must notify a Personal Data breach that relates to Personal Data Processed in the context of the Service to the other Party, without undue delay, and no later than 48 hours after having become aware of a Personal Data Breach. MontyPay will provide reasonable assistance to Merchant in complying with its obligations to notify a Personal Data Breach.

7.4 The Parties will use their best efforts to reach an agreement on whether and how to notify a Personal Data Breach, and must document all Personal Data Breaches, including the facts relating to the Personal Data Breach, its effects and the remedial action taken.

8. LIABILITY TOWARDS DATA SUBJECTS

Subject to the liability clauses in the PSA, the Parties agree that they will be held liable for violations of Data Protection Law towards Data Subjects as follows:

- (a) Merchant is responsible for the damage caused by the Processing which infringes Data Protection Law or this Agreement.
- (b) When MontyPay acts as a Processor, it will be liable for the damage caused by the Processing only where it has not complied with obligations of Data Protection Law specifically directed to Processors or where it has acted outside of or contrary to Merchant's lawful instructions. In that context, MontyPay will be exempt from liability if it proves that it is not in any way responsible for the event giving rise to the damage.
- (c) Where the Parties are involved in the same Processing and where they are responsible for any damage caused by the Processing, both Merchant and MontyPay may be held liable for the entire damage in order to ensure effective compensation of the Data Subject. If MontyPay paid full compensation for the damage suffered, it is entitled to claim back from Merchant that part of the

compensation corresponding to Merchant's part of responsibility for the damage.

9. LIABILITY – CHOICE OF LAW AND RESOLUTION OF DISPUTES

9.1 This Agreement and any dispute or claim arising out of or in connection with this Agreement shall be governed by and construed in accordance with the law of England and Wales.

9.2 For the benefit of MontyPay, the parties irrevocably agree that the courts of England and Wales shall have exclusive jurisdiction to hear, settle and/or determine any dispute, controversy or claim (including any non-contractual dispute, controversy or claim) arising out of or in connection with this Agreement, including any question regarding its existence, validity, formation or termination. For these purposes, each party irrevocably submits to the jurisdiction of the England and Wales courts. However, nothing in this Clause 9.2 limits the right of MontyPay to bring proceedings, including third party proceedings, against Merchant in any other court of competent jurisdiction, and the bringing or continuing of proceedings in any one or more jurisdictions shall not preclude the bringing of proceedings in any other jurisdiction, whether concurrently or not, if and to the extent permitted by applicable Law.

9.3 Notwithstanding the liability from direct losses neither Party will be liable for any indirect or consequential damages of the other Party, such as (but not limited to) loss of revenue, loss of profit, loss of opportunity and loss of goodwill. No limitation of liability shall apply in case of gross negligence or wilful intent.

10. EFFECTIVE DATE AND TERMINATION

10.1 This Agreement shall become effective on the Effective Date as such term is defined in the Fee Schedule.

10.2 This Agreement will remain in effect for the duration of the PSA. The termination of the PSA will result in the termination of this Data Processing Agreement.

10.3 However, Data Processor remains subject to the obligations stipulated in this DPA and applicable data protection law, as long as Data Processor processes Customer Personal Data on behalf of Data Controller.

10.4 In the event of the termination of this DPA, Data Controller is entitled to determine the media format to be used by Data Processor when returning Customer Personal Data and to determine if Customer Personal Data should instead be deleted.

11. CONFLICT

11.1 If there is any conflict between the provisions of this DPA and the provisions of the PSA regarding Personal Data Processing, the provisions of this DPA will prevail.