DATA PROCESSING AGREEMENT

Last updated: January 1, 2024

This Data Processing Agreement ("**DPA**") regulates the Processing of Personal Data subject to Applicable Data Protection Law in the context of each agreement and/ or statement of work which references this DPA or to which this DPA is attached (the "**Agreement**") between

(i) the Mastercard entity which is a party to the Agreement,
(ii) and if not already a Party to the Agreement, to the least extent necessary under Europe Data Protection Law where applicable to Mastercard under this DPA, Mastercard Europe SA, a Belgian private limited liability company, with Belgian enterprise number RPR 0448038446, whose registered office is at 198/A, Chaussée de Tervuren, 1410 Waterloo, Belgium (together "**Mastercard**"); and
(iii) the Merchant, Issuer or other applicable counterparty (the "**Customer**").

Mastercard and Customer are hereinafter collectively referred to as "the Parties" or each individually as a "Party."

Definitions

"Affiliate" means in relation to a Party, any other entity which directly or indirectly Controls, is Controlled by, or is under direct or indirect common Control with that Party from time to time. "Control", for the purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

"Applicable Data Protection Law" means all applicable international, federal, state, provincial, and local laws, rules, regulations, directives, and governmental requirements relating in any way to the privacy, confidentiality, protection, transfer, or security of Personal Data, including, without limitation: Europe Data Protection Law; the Gramm-Leach-Bliley Act; the U.S. State Privacy Laws; the Brazil General Data Protection Act, Law n° 13.709/2018; laws regulating unsolicited email, telephone, and text message communications; security breach notification laws; laws imposing minimum security requirements; laws requiring the secure disposal of records containing certain Personal Data; laws governing the portability and/or cross-border transfer of Personal Data; and all other similar international, federal, state, provincial, and local requirements, each as applicable and as amended from time to time.

"**Controller**" means "Controller," "Business," or an analogous term as defined in Applicable Data Protection Law.

"**Data Subject**" means a natural person whose Personal Data is Processed in the context of the Agreement.

"**Data Subject Rights**" means all rights granted to Data Subjects under Applicable Data Protection Law, which may include—depending on Applicable Data Protection Law—the right to know, the right of access, rectification, erasure, complaint, data portability, restriction of Processing, objection to the Processing, and rights relating to automated decision-making.

"**Disclosure Request**" means any request by a Government Agency for access to, or disclosure of, Personal Data for law enforcement, national security, regulatory reporting or other purposes.

"**Europe**" means the European Economic Area ("EEA"), Monaco, Switzerland and the United Kingdom.

"**Europe Data Protection Law**" means GDPR and the e-Privacy Directive 2002/58/EC (as amended by Directive 2009/136/EC) and any legislation and/or regulation implementing or made pursuant to them in any country in the EEA; the UK Data Protection Law; the Swiss Federal Data Protection Act and implementing ordinances (the "FADP"); and the Monaco Data Protection Act; and any legislation and/or regulation which amends, replaces, re-enacts or consolidates any of them.

"**GDPR**" means the EU General Data Protection Regulation 2016/679 (as amended and replaced from time to time).

"**Government Agency**" means any competent public or quasi-public authority (including without limitation regulators, local government authorities, law enforcement authorities and national security agencies) of any jurisdiction that may request disclosure of Personal Data Processed in connection with the Services.

"**Mastercard BCRs**" means the Mastercard Binding Corporate Rules as approved by the EEA data protection authorities and the UK Information Commissioner's Office and available at https://www.mastercard.us/content/dam/mccom/global/documents/mastercard-bcrs.pdf.

"**Mastercard Rules**" means the Rules for the Mastercard, Maestro, and Cirrus brands, as available at https://www.mastercard.us/en-us/business/overview/support/rules.html.

"**Participating Members**" means Mastercard customers that participate in the Services, and may process Customer Personal Data for the purpose of enabling the Services under and pursuant to the terms of the Agreement. For the avoidance of doubt, where Customer is an issuer, Customer Personal Data may be shared with participating merchant members and where Customer is a merchant, Customer Personal Data may be shared with participating issuer members.

"**Personal Data**" means any information provided by Customer to, or which is collected on behalf of Customer by, Mastercard to provide services to Customer pursuant to the Agreement: (i) relating to an identified or identifiable natural person or (ii) that is otherwise defined as "Personal Data," "Personal Information," or an analogous term in Applicable Data Protection Law.

"**Processing of Personal Data**" (or **"Process/Processed"**) means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as access, 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 "Processor," "Service Provider," "Contractor," or an analogous term as defined in Applicable Data Protection Law.

"**Sale**" and "**Selling**" have the meaning defined in the U.S. State Privacy Laws.

"**Share**," "**Shared**," and "**Sharing**" have the meaning defined in the CCPA.

"**Standard Contractual Clauses**" means the clauses annexed to the EU Commission Implementing Decision 2021/914 of June 4, 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 (OJ L 199, 7.6.2021, p. 31-61), as amended or replaced from time to time. In respect of Personal Data to which the FADP applies, the Standard Contractual Clauses has the same meaning, as adapted to satisfy the requirements set out by the Swiss Federal Data Protection and Information Commissioner as per Section 13.6 of this DPA.

"**U.S. State Privacy Laws**" means any state Privacy and Data Protection Laws of the United States ("U.S.") applicable to Mastercard's Processing of Personal Data to provide the Services to Customer, which include but are not limited to: (i) the California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 et seq., as amended by the California Privacy Rights Act of 2020, and their implementing regulations ("CCPA"); (ii) Colorado Privacy Act, Colorado Rev. Stat. §§ 6-1-1301 to 6-1-1313 ("ColoPA"); (iii) Connecticut Personal Data Privacy and Online Monitoring Act, Public Act No. 22-15) ("CPOMA"); (iv) Utah Consumer Privacy Act (Utah Code Ann. §§ 13-61-101 to 13-61-404) ("UCPA"); and (v) Virginia Consumer Data Protection Act, Virginia Code Ann. §§ 59.1-575 to 59.1-585 ("VCDPA"), all as amended from time to time.

"**Sub-processor**" means a Processor engaged by Mastercard to Process Personal Data.

"**Supervisory Authority**" means the competent supervisory authority under Applicable Data Protection Law.

"**UK Addendum**" means the addendum to the Standard Contractual Clauses issued by the UK Information Commissioner under Section 119A of the UK Data Protection Act 2018 (version B1.0, in force March 21, 2022).

"UK Data Protection Law" means (i) the Data Protection Act 2018; (ii) the GDPR as amended by the Data Protection Act 2018 and the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 and 2020 ("UK GDPR") as relevant; and (iii) the e-Privacy Directive 2002/58/EC (as amended by Directive 2009/136/EC) as transposed into UK national law, all as amended from time to time.

Capitalized terms used but not defined herein have the meanings given to them in the applicable Agreement.

1. Scope and applicability

1.1. This DPA applies to the Processing of Personal Data subject to Applicable Data Protection Law by Mastercard in the context of the applicable Agreement.

1.2. This DPA forms part of the Agreement between Mastercard and Customer and prevails over any conflicting term of the applicable Agreement but does not otherwise modify the applicable Agreement.

1.3. For the purposes of this DPA only and except where indicated otherwise, the term "Party" shall include each Party's respective Affiliates insofar as they are a Party to the Agreement and/or any collateral thereto.

1.4. The subject matter, nature, purpose and duration of the Processing, the types of Personal Data and categories of Data Subjects are set out in Attachment 1 to the DPA.

2. Roles and Obligations of the Parties

2.1. The Parties represent and warrant that they will comply with Applicable Data Protection Law when Processing Personal Data in the context of the Services. The Parties shall notify each other within a reasonable time if they can no longer meet their obligation under Applicable Data Protection Law. Upon receiving notice, each Party may direct the other to take steps as reasonable and appropriate to remediate unauthorized use of Personal Data.

2.2. Mastercard is a Processor Processing Personal Data on behalf and upon instructions of Customer for the provision of the Services. Customer further acknowledges that Mastercard is also a Processor acting on behalf of Participating Members for the provision of the Services. For the avoidance of doubt, Mastercard's relationship with the Customer is independent from its contractual relationships with Participating Members. In particular, Customer understands and agrees that Mastercard Processes Personal Data to provide services to Participating Members and Mastercard may disclose Customer Personal Data to the Participating Members in connection with the Services.

2.3. Customer acknowledges that Mastercard may Process Personal Data as a Controller relating to the operation, support, or use of the Services, including to share aggregated data with prospective Participating Members for the purpose of enabling the resolution of the disputes or the queries on transactions, and for Mastercard's other business purposes as set out in Attachment 3 of this DPA.

2.4. For the avoidance of doubt, the obligations imposed on Controllers or Processors under this DPA apply irrespective of whether Applicable Data Protection Law uses the terms Controller and Processor, or uses similar terms, and irrespective of whether it provides or not for a distinction between Controllers and Processors.

2.5. Solely for the purpose of U.S. State Privacy Laws, where applicable:

2.5.1. Notwithstanding Sections 2.2 to 2.4 above, and solely for the purposes of U.S. State Privacy Laws, the Parties acknowledge and agree that Customer is a Controller and appoints Mastercard as a Processor to Process Personal Data on behalf of Customer.

2.5.2. Mastercard will Process Personal Data in accordance with the Agreement, this DPA, and as permitted by U.S. State Privacy Laws. Except as otherwise permitted by applicable U.S. State Privacy Laws, Mastercard will not (i) retain, use, or disclose Personal Data for any purpose other than for the purpose of performing the Services as specified in Attachment 1 to this DPA, (ii) retain, use, or disclose Personal Data outside of the direct business relationship between the Parties; (iii) Sell or Share Personal Data; (iv) combine the Personal Data with other Personal Data obtained from, or on behalf of, sources other than the Customer; and (v) further collect Personal Data.

2.5.3. The Parties acknowledge and agree that the exchange of Personal Data between the Parties does not form part of any monetary or other valuable consideration exchanged between the Parties with respect to the Agreement or this DPA.

2.5.4. Notwithstanding any provision to the contrary of the Agreement or this DPA, the terms of this Section 2.5 of the DPA shall not apply to Mastercard's Processing of Personal Data that is exempt from applicable U.S. State Privacy Laws.

3. Legal Ground and Notice

3.1. Customer must rely on a valid legal ground, and must ensure that Data Subjects are properly informed in accordance with Applicable Data Protection Law relating to the Processing of the Personal Data, including the transfer to or access of Processors located outside of the country of origin of the Personal Data, or otherwise Processing of Personal Data in the context of the Services and the ways in which their Personal Data will be Processed by Customer and Mastercard. In particular, Customer confirms and warrants that it will obtain consent for the collection, use, disclosure, transfers and any other Processing of Personal Data by Customer and Mastercard as set out in the Agreement and this DPA, to the extent and in the manner required by Applicable Data Protection Law.

3.2. Upon request from Mastercard, Customer must demonstrate that it relies on a valid legal ground for the Processing, including consent, where applicable.

4. Instructions

4.1. Customer's instructions are documented in this DPA and the applicable Agreement.

4.2. Customer may reasonably issue additional instructions as necessary to comply with Applicable Data Protection Law.

4.3. Unless prohibited by applicable law, Mastercard will inform Customer if Mastercard is subject to a legal obligation that requires Mastercard to Process Personal Data in contravention of Customer's documented instructions.

4.4. Customer hereby instructs Mastercard to Process Personal Data as necessary to provide the Services, acknowledging and agreeing that (i) Mastercard may transfer Personal Data to countries outside the country of origin for operational or organizational reasons in the course of providing its Services; and (ii) there is a risk that such Personal Data may be subject to a Disclosure Request or other access by a Government Agency in the recipient country.

4.5. As between the Customer and Mastercard, it shall be the Customer that is solely responsible for evaluating and, where Europe Data Protection Law, if applicable, requires documentation, documenting the level of

protection afforded to Personal Data in any country outside the country of origin where Personal Data is transferred in the context of the Agreement, provided that Mastercard shall, upon reasonable request of the Customer, taking into account the nature of the Processing and the information available to Mastercard, provide commercially reasonable assistance to the Customer in conducting and documenting its assessment.

5. Personnel

Mastercard will ensure that all personnel authorized to Process Personal Data are subject to an obligation of confidentiality.

6. Information Security

6.1. The Parties shall develop, maintain and implement a comprehensive written information security program designed to ensure a level of security appropriate to the risk and compliance with Applicable Data Protection Law. 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.

6.2. Without limitation, each Party's information security program shall include technical, physical, and administrative/organizational safeguards designed to (1) ensure the security and confidentiality of Personal Data; (2) protect against any anticipated threats or hazards to the security and integrity of Personal Data; and (3) protect against any actual or suspected unauthorized Processing, loss, use, disclosure or acquisition of or access to any Personal Data Processed in connection with the Services ("Information Security Incident").

6.3. Each Party's information security program shall, among other things, include regular testing or otherwise monitoring of the effectiveness of its information safeguards. In addition, each Party shall comply with all provisions of its written information security policies, procedures and guidelines which the Parties have mutually agreed are applicable to the Services under this Agreement.

6.4. Notwithstanding Sections 6.1 to 6.3 above, where the Processing takes place in Europe or concerns Personal Data gathered in Europe, the Parties shall implement and maintain the technical and organizational measures listed in Attachment 2 to this DPA, as appropriate.

7. Information Security Incident

7.1. To the extent required by Applicable Data Protection Law, each Party shall inform the other Party in writing of any Information Security Incident involving Personal Data that has been Processed in connection with the Services in a commercially reasonable time frame, and in any event, no later than 48 hours after becoming aware of the Information Security Incident.

7.2. Such Information Security Incident notice shall describe, in reasonable detail, the nature of the Information Security Incident, the data elements involved, the identities of the affected individuals (if known), and the corrective action taken or to be taken to remedy the Information Security Incident.

7.3. Customer shall be solely responsible for any filings, communications, notices, press releases, or reports related to any Information Security Incident involving Personal Data processed by Customer or Mastercard in the context of the Services. Mastercard will provide reasonable assistance to Customer in complying with its obligations to notify an Information Security Incident.

7.4. Except to the extent prohibited by applicable legal, regulatory or law enforcement requirements, Customer shall obtain Mastercard's approval prior to the publication or communication of any filings, communications,

notices, press releases or reports related to any Information Security Incident that expressly mentions Mastercard or its Affiliates.

8. Sub-processing

8.1. Customer hereby provides a general authorization for Mastercard to engage Sub-processors in the context of the Services.

8.2. Mastercard represents and warrants it:

8.2.1. Binds its internal Sub-processors to comply with the Customer's instructions and to respect the Mastercard BCRs.

8.2.2. Requires its external Sub-processors, via a written agreement, to comply with the requirements of Applicable Data Protection Law applicable to Processors and data transfers, with the Customer's instructions and with the same obligations as are imposed on Mastercard by this DPA and the Mastercard BCRs, including sub-processing and audit requirements set forth in the Mastercard BCRs.

8.2.3. Remains liable to the Customer for the performance of its Sub-processors' obligations.

8.2.4. Commits to provide a list of Sub-processors to Customer upon request.

8.2.5. Will inform Customer of any addition or replacement of a Sub-processor in a timely fashion so as to give Customer an opportunity to object to the change or terminate the DPA on reasonable grounds, before the Personal Data is communicated to the new Sub-processor. In the event Customer objects, the Parties shall discuss Customer's concerns in good faith with a view to achieving a commercially reasonable resolution.

9. Assistance

9.1. Taking into account the nature of the Processing, and the information available to Mastercard, Mastercard will assist Customer, including, as appropriate, by implementing technical and organizational measures, with the fulfilment of Customer's own obligations under Applicable Data Protection Law, and provide to Customer all information available to Mastercard as necessary to demonstrate compliance with Customer's own obligations under Applicable Data Protection Law, including Customer's obligation to comply with Data Subjects' requests to exercise Data Subject Rights, conduct data protection impact assessments and prior consultations with Supervisory Authorities.

9.2. Mastercard will maintain records of Processing of Personal Data as required by Applicable Data Protection Law.

9.3. Mastercard will notify Customer when local laws prevent Mastercard from fulfilling its obligations under this DPA or the Mastercard BCRs and have a substantial adverse effect on the guarantees provided by this DPA or the Mastercard BCRs.

10. Data Subject Rights Requests

10.1. Customer represents and warrants that Customer's process for handling Data Subjects' requests to exercise Data Subject Rights complies with Applicable Data Protection Law.

10.2. Customer shall be solely responsible for responding to Data Subjects' requests to exercise Data Subject Rights. Mastercard will notify Customer of any such requests that Mastercard receives.

10.3. Mastercard shall not be required to delete any Customer Personal Data to comply with a Customer's request directed by Customer if Mastercard's retention of such information is required under any Applicable Data Protection Law.

11. Audit

11.1. To the extent required by Applicable Data Protection Law, no more than once in any 12-month rolling period, Mastercard must make available to Customer all information necessary to demonstrate compliance with the obligations of this DPA and allow for and contribute to audits, including inspections, as mandated by a Supervisory Authority or reasonably requested in writing by Customer and performed by a qualified and independent auditor as agreed upon by Customer and Mastercard, subject to the strictest confidentiality obligations.

11.2. Mastercard and Customer each bear their own costs related to an audit under this Section 11.

12. Governmental Requests for Personal Data

12.1. Except to the extent prohibited by applicable legal, regulatory or law enforcement requirements, each Party shall:

12.1.1. Promptly inform the other Party in writing if any Government Agency makes a Disclosure Request for Personal Data that has been Processed in connection with the Services; and

12.1.2. Without limiting its rights under applicable law, cooperate with the other Party as reasonably necessary to comply with any direction or ruling made by such Government Agencies.

12.2. Where Mastercard is requested to disclose to a Government Agency Personal Data that Mastercard is Processing, Mastercard will only comply with such request in accordance with the Mastercard BCRs and Applicable Data Protection Law. Mastercard will refer the Government Agency to the Customer, unless Mastercard is prohibited from doing so by applicable legal, regulatory or law enforcement requirements.

13. International Data Transfers

13.1. Customer authorizes Mastercard to Process Personal Data in accordance with Applicable Data Protection Law in locations outside of the country where the Customer is located (including Canada, India, Ireland and the U.S.) and/or where the Data Subjects are located for the provision of the Services.

13.2. To the extent the Processing of Personal Data is subject to Europe Data Protection Law, Customer authorizes Mastercard to transfer Personal Data Processed in connection with the Services outside of Europe, including into the U.S. and India, in accordance with the Mastercard BCRs or with any other lawful data transfer mechanism that provides an adequate level of protection under Europe Data Protection Law. Mastercard represents and warrants that it will abide by the Mastercard BCRs when Processing Personal Data under this DPA.

13.3. The text from module four of the Standard Contractual Clauses shall be incorporated by reference to this DPA and apply to Personal Data subject to Europe Data Protection Law exported to a Customer based in a country outside the country of origin that is not deemed to provide an adequate level of protection under Europe Data Protection Law, where Mastercard is the Processor and Customer is the Controller.

13.4. For the purposes of the Standard Contractual Clauses, the following shall apply:

13.4.1. The “data exporter” is Mastercard; the “data importer” is the Customer;
13.4.2. Clause 7 applies;
13.4.3. Clause 9 (Use of sub-processors) (a) option 2: as specified in Section 8 of this DPA;
13.4.4. The optional paragraph in Clause 11(a) is removed;
13.4.5. Clause 13(a): first option applies;

13.4.6. Clause 17 (Governing law): the clauses shall be governed by the laws as specified in Section 16 of this DPA;

13.4.7. Clause 18 (Choice of forum and jurisdiction): the courts shall have jurisdiction, as specified in Section 16 of this DPA;

13.4.8. The information as required by Annex I of the Standard Contractual Clauses is as set out in Attachment 1 to this DPA and the signatures for the purpose of Annex I of the Standard Contractual Clauses are the signatures to the Agreement and the date is the date of the Agreement; and

13.4.9. The technical and organizational measures required by Annex II of the SCCs are as set out in Attachment 2 to this DPA.

13.5. The parties agree that the UK Addendum is incorporated by reference in this DPA and modifies the Standard Contractual Clauses as set out in such standard data protection clauses in respect of any transfer of Personal Data made under the Agreement by Mastercard to Customer to a country that is not recognized as adequate under UK adequacy regulations. Part 1 of the UK Addendum is completed as follows: (i) in Table 1, the "Exporter" is Mastercard and the "Importer" is Customer, their details are set forth in this DPA and the Agreement; (ii) in Table 2, the first option is selected and the "Approved EU SCCs" are the Standard Contractual Clauses referred to in Section 13.3 of this DPA; (iii) in Table 3, Annex 1 (A and B) to the "Approved EU SCCs" is Attachment 1 to this DPA respectively; and (iv) in Table 4, both the "Importer" and the "Exporter" can terminate the UK Addendum.

13.6. The parties agree that if the Personal Data transfer made under the Agreement by Mastercard to Customer to a country that is not recognized as adequate by Switzerland, is governed by the FADP only (and not also the GDPR), the following shall apply: (i) in deviation of Clause 17 of the Standard Contractual Clauses, the Standard Contractual Clauses shall be governed by and construed in accordance with the substantive laws of Switzerland; (ii) in deviation of Clause 18(a) and (b) of the Standard Contractual Clauses, any disputes arising from the Standard Contractual Clauses shall be subject to the exclusive jurisdiction of the ordinary Courts of Zurich, canton of Zurich, Switzerland; and (iii) the references to the GDPR and specific articles thereof in the Standard Contractual Clauses should be interpreted as references to the FADP and its corresponding provisions, as applicable. In any event (i.e. if the Personal Data transfer concerned is governed by the FADP and also the GDPR), (a) in supplementation of Clause 8.7 of the Standard Contractual Clauses, the term "sensitive data" shall include data on the intimate sphere, trade union related views or activities, political, religious or philosophical activities, criminal proceedings, administrative proceedings and sanctions and social security measures; and (b) the term "Member Sate" as used in the Standard Contractual Clauses must not be interpreted in such a manner as to exclude Data Subjects in Switzerland from the possibility of bringing legal proceedings against the data exporter and/or data importer in their place of habitual residence (Switzerland). Clause 18 (c) of the Standard Contractual Clauses shall be interpreted accordingly.

13.7. If Mastercard's compliance with Europe Data Protection Law applicable to international data transfers is affected by circumstances outside of Mastercard's control, including if a legal instrument for international data transfers is invalidated, amended, or replaced, then Customer and Mastercard will work together in good faith to reasonably resolve such non-compliance.

13.8. In the event Mastercard is compelled to comply with a Disclosure Request and such disclosure causes Customer to breach Europe Data Protection Law, Customer represents and warrants that it will not hold Mastercard liable for such disclosure. Customer further agrees that - to the greatest extent authorized by applicable law - it will not revoke or amend its instruction to Process Personal Data as set out in this DPA and the Agreement, unless strictly required by Europe Data Protection Law. Any amendments to Customer's instructions to Process Personal Data, such as where necessary to ensure the continued compliance with Europe Data Protection Law, must be agreed by both parties in writing prior to taking effect.

14. Notifications

Customer will send all notifications, requests and instructions pertaining to this DPA in accordance with the notice provision contained in the Agreement with a copy provided to Mastercard's Privacy and Data Protection department via email to privacyanddataprotection@mastercard.com. Please include "Ethoca customer" as the subject of the email so that the request can be routed appropriately.

15. Liability

To the extent permitted by applicable law, where Mastercard has paid compensation, damages or fines under Applicable Data Protection Law, Mastercard is entitled to claim back from Customer that part of the compensation, damages or fines, corresponding to Customer's part of responsibility for the compensation, damages or fines.

16. Applicable Law and Jurisdiction

16.1. To the extent the Processing of Personal Data is subject to:

16.1.1. GDPR, this DPA and the Processing of Personal Data will be governed by the law of Belgium and any dispute will be submitted to the Courts of Brussels;

16.1.2. UK Data Protection Law, this DPA and the Processing of Personal Data will be governed by UK law and any dispute will be submitted to the Courts of England and Wales;

16.1.3. FADP and implementing ordinances, this DPA and the Processing of Personal Data will be governed by substantive Swiss law and any dispute will be submitted to the exclusive jurisdiction of the ordinary Courts of Zurich, canton of Zurich, Switzerland; and

16.2. To the extent the Processing of Personal Data is not subject to the above Europe Data Protection Laws, this DPA and the Processing of Personal Data will be governed by the law applicable to the Agreement as specified in the Agreement, and any dispute will be submitted to the courts specified in the Agreement.

17. Termination and return or deletion

17.1. This DPA is terminated when there are no further active Agreements in place between Mastercard and the Customer.

17.2. When the DPA expires or upon termination of the DPA or upon a request to delete or return Personal Data by Customer, except for any Personal Data which Mastercard Processes as a Controller, Mastercard will, at the choice of Customer, delete, anonymize, or return such Personal Data to Customer, 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 Mastercard will protect the confidentiality of the Personal Data and will not actively Process the Personal Data anymore).

18. Invalidity and severability

If any provision of this DPA is found by any court or administrative body of a competent jurisdiction to be invalid or unenforceable, then the invalidity or unenforceability of such provision does not affect any other provision of this DPA and all provisions not affected by such invalidity or unenforceability will remain in full force and effect.

ATTACHMENT 1

A. LIST OF PARTIES

Data exporter:

- **Name**: Mastercard as defined above
- **Address**: As set forth in the Agreement. For UK Data Transfer, Mastercard Europe Services Limited, 10 Upper Bank Street, Canary Wharf, London, E14 5NP, United Kingdom
- **Contact person's name, position and contact details**: As set forth in the Agreement
- **Activities relevant to the data transferred under these Clauses**: Providing the Services as described in this DPA and the Agreement
- **Data protection officer (if applicable)**: Europe Data Protection Officer, privacyanddataprotection@mastercard.com
- **Representative in the European Union**: N/A
- **Representative in the UK (where Clause 3 applies)**: N/A
- **Activities relevant to the data transferred under the SCCs**: The receipt of the Services under the Agreement.
- **Role (Controller/Processor)**: Processor

Data importer:

- **Name**: Customer as defined above
- **Address**: As set forth in the Agreement
- **Contact person's name, position and contact details**: As set forth in the Agreement
- **Activities relevant to the data transferred under these Clauses**: Receiving the Services as described in the Agreement
- **Role (Controller/Processor)**: Controller

B. DESCRIPTION OF THE PROCESSING/TRANSFER

1. **Data Subjects**. The Personal Data Processed concern the following categories of Data Subjects:

    (a) Cardholders

    (b) Issuer's representatives

    (c) Merchant's representatives

    (d) Sole proprietors

2. **Categories of Personal Data**. The Personal Data Processed concern the following categories of data:

    (a) Transaction-related information such as card or account number (full or partial), transaction type, currency and amount, transaction date and time, information about the disputed or queried transaction and its outcome, items purchased, history of the account, merchant order number, cardholder information such as name, address, phone number, IP address, email address location, merchant identifier, as applicable under the Agreement, and any other types of Personal Data listed in the Agreement.

    (b) Information of Issuer's or Merchant's representatives such as user ID, name, role, email, phone, as applicable.

    (c) The Processing performed under the DPA does not include Processing of special categories of data.

3. **Frequency of transfer**. On a continuous basis.

4. **Nature of Processing**. Mastercard performs collection, storage, deletion, disclosure, monitoring, reporting, data analysis and data aggregation as reasonably necessary for the purpose of providing the Services.

5. **Purpose of Processing**. The subject-matter of the Processing under this DPA is the provision of the Services set out in the applicable Agreement.

6. **Duration of the Processing.** Personal Data will be retained for as long as necessary taking into account the purpose of the Processing, and in compliance with applicable laws, including laws on the statute of limitations and Applicable Data Protection Law.

7. **Transfer to Sub-processors**. The Personal Data may be transferred to Sub-Processors to provide the Services as described in this DPA and the Agreement.

C. COMPETENT SUPERVISORY AUTHORITY

Belgian Data Protection Authority (except in respect of Personal Data to which (i) the UK GDPR applies, in which case, the UK Information Commissioner's Office and (ii) the FADP applies, in which case, the Swiss Federal Data Protection and Information Commissioner).

ATTACHMENT 2
SECURITY MEASURES

The Parties will, as a minimum, implement the following types of security measures:

1. Physical access control

Technical and organizational measures to prevent unauthorized persons from gaining access to the data processing systems available in premises and facilities (including databases, application servers and related hardware), where Personal Data are processed, include:

- Establishing security areas, restriction of access paths;
- Establishing access authorizations for employees and third parties;
- Access control system (ID reader, magnetic card, chip card);
- Key management, card-keys procedures;
- Door locking (electric door openers etc.);
- Security staff, janitors;
- Surveillance facilities, video/CCTV monitor, alarm system;
- Securing decentralized data processing equipment and personal computers.

2. Virtual access control

Technical and organizational measures to prevent data processing systems from being used by unauthorized persons include:

- User identification and authentication procedures;
- ID/password security procedures (special characters, minimum length, change of password);
- Automatic blocking (e.g. password or timeout);
- Monitoring of break-in-attempts and automatic turn-off of the user ID upon several erroneous passwords attempts;
- Creation of **one** master record per user, user master data procedures, per data processing environment.

3. Data access control

Technical and organizational measures to ensure that persons entitled to use a data processing system gain access only to such Personal Data in accordance with their access rights, and that Personal Data cannot be read, copied, modified or deleted without authorization, include:

- Internal policies and procedures;
- Control authorization schemes;
- Differentiated access rights (profiles, roles, transactions and objects);
- Monitoring and logging of accesses;
- Disciplinary action against employees who access Personal Data without authorization;
- Reports of access;
- Access procedure;
- Change procedure;
- Deletion procedure.

4. Disclosure control

Technical and organizational measures to ensure that Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media (manual or electronic), and that it can be verified to which companies or other legal entities Personal Data are disclosed, include:

- Tunneling;
- Logging;
- Transport security.

5. Entry control

Technical and organizational measures to monitor whether data have been entered, changed or removed (deleted), and by whom, from data processing systems, include:

- Logging and reporting systems;
- Audit trails and documentation.

6. Control of instructions

Technical and organizational measures to ensure that Personal Data are processed solely in accordance with the Instructions of the Controller include:

- Unambiguous wording of the contract;
- Formal commissioning (request form);
- Criteria for selecting the Processor.

7. Availability control

Technical and organizational measures to ensure that Personal Data are protected against accidental destruction or loss (physical/logical) include:

- Backup procedures;
- Mirroring of hard disks (e.g. RAID technology);
- Uninterruptible power supply (UPS);
- Remote storage;
- Anti-virus/firewall systems;
- Disaster recovery plan.

8. Separation control

Technical and organizational measures to ensure that Personal Data collected for different purposes can be processed separately include:

- Separation of databases;
- “Internal client” concept / limitation of use;
- Segregation of functions (production/testing);
- Procedures for storage, amendment, deletion, transmission of data for different purposes.

ATTACHMENT 3
MASTERCARD BUSINESS PURPOSES

Mastercard may process the Personal Data for the following additional purposes:

1. For the benefit of the Cardholder supplying the Customer Personal Data to support the Services;

2. As may be appropriate to Mastercard's staff, accountants, auditors, or counsel;

3. As may be required or requested by any judicial process or governmental agency having or claiming to have jurisdiction over Mastercard;

4. For accounting, auditing, billing, reconciliation, and collection activities;

5. For the purpose of processing and/or resolving chargebacks or other disputes;

6. For the purpose of protecting against or preventing actual or potential fraud, unauthorized transactions, claims, or other liability, including to third parties providing these services;

7. For the purpose of managing risk exposures, franchise quality, and compliance with Mastercard Rules (as applicable);

8. For product development and improvement purposes, and providing products or services to customers or other third parties, except that any Customer Personal Data provided in such product or services will only be provided to the Customer and will consist solely of the Customer Personal Data provided by the Customer to Mastercard;

9. For preparing internal reports for use by Mastercard staff, management, and consultants for the purposes of operating, evaluating, and managing its business;

10. For preparing and furnishing compilations, analyses, and other reports of aggregated information, and anonymizing Customer Personal Data, provided that such compilations, analyses, or other reports do not identify any (a) customer other than the customer for which Mastercard prepares the compilation, analysis, or other report, or (b) Cardholder whose transactions were involved in the preparation of any such compilation, analysis, or other report;

11. For the purposes of complying with applicable legal requirements; or

12. For other purposes for which consent has been provided by the individual to whom the Personal Data relates.

The rights to process Personal Data for the above purposes shall also apply to Mastercard's Affiliates, including Mastercard International Incorporated if not already a Party to the Agreement.