MASTERCARD DATA PROCESSING AGREEMENT

CONTROLLER TO PROCESSOR SPECIFIC TERMS AND CONDITIONS

Last Updated: 15th May, 2024

1. **Privacy and Data Protection.**

This Data Processing Agreement ("**Data Processing Agreement**") supplements the Master Supplier Agreement (the "**Agreement**") between Mastercard and Supplier and governs Supplier's Processing of Mastercard Personal Data. This Data Processing Agreement is intended to satisfy legal requirements under Privacy and Data Protection Law. If Supplier or any Supplier Personnel receives, has access to or otherwise Processes Personal Data, Supplier shall comply with the requirements of this Data Processing Agreement.

The terms used in this Data Processing Agreement have the meaning set forth in this Data Processing Agreement. Capitalized terms not otherwise defined herein have the meaning given to them in the Agreement. Except as modified below, the terms of the Agreement remain in full force and effect. Addendum A1, Appendix 1 and Appendix 2 form an integral part of this Data Processing Agreement.

2. **Definitions.**

In this Data Processing Agreement, the following definitions apply:

"**Business Purpose**" means the use of Personal Data for Mastercard or Supplier's operational purposes, or other notified purposes as agreed under this Agreement or specified in the SoW, provided that the use of Personal Data is reasonably necessary and proportionate to achieve the operational purpose for which the Personal Data was collected or processed or for another operational purpose that is compatible with the context in which the Personal Data was collected.

"**Data Protection Rights**" means all rights granted to individuals under the applicable Privacy and Data Protection Law, including but not limited to the right to know, the right of access, reproduction, supplement, rectification, or erasure to or of Personal Data, the right to raise complaints, the rights relating to data portability, restriction on Processing, and objection to the Processing (including the right to withdraw consent) and the rights relating to automated decision-making.

"Europe" means the European Economic Area, Switzerland, Monaco and the United Kingdom.

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

"Government Body" means (1) the government of a country or of a political subdivision of a country, (2) an instrumentality of any such government, (3) any other individual, entity, or organization authorized by Law to perform any executive, legislative, judicial, regulatory, administrative, military, or police functions of any such government, and (4) an intergovernmental organization.

"**Government Agency"** means any public and quasi-public authority that may have jurisdiction over Mastercard or Supplier to request for Personal Data.

"Law" means one or more laws, statutes, regulations, rules, executive orders, conventions, and other legally binding official releases of or by any Government Body, in each case as then in effect in the territory where the obligations under this Agreement and the applicable SOWs are being carried out.

"**Personal Data**" or "**Personal Information**" (which may be used interchangeably in this Agreement) means any information relating to an identified or identifiable individual, whether directly or indirectly identifiable, including but not limited to contact information, demographic information, passport number, Social Security number or other national identification number, bank account information, Primary Account Number and authentication information (e.g. identification codes, passwords) or as defined under the applicable Privacy and Data Protection Law.

"**Personal Data Breach"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, access to, or other unauthorized Processing of Personal Data transmitted, stored, or otherwise Processed.

"**Pre-2021 Standard Clauses**" or "**Pre-2021 SCCs**" means

(i) the standard contractual clauses for the transfer of personal data to data processors established in third countries adopted by the European Commission decision of 5 February 2010, published under document number C(2010) 593 2010/87/EU;
(ii) the standard contractual clauses for the transfer of personal data to third countries adopted by the European Commission decision of 15 June 2001, published under document number C(2001) 1539); and
(iii) the standard contractual clauses for the transfer of personal data to third countries adopted by the European Commission decision of 27 December 2004, published under document number C(2004) 5271 (as applicable)

"Privacy and Data Protection Law" means any Law, statute, declaration, decree, legislation, enactment, order, ordinance, regulation, rule, circular, national, local or industry standard (as amended and replaced from time to time) which relates to the protection of individuals with regards to the Processing of Personal Data to which the Parties are subject, including but not limited to (1) 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 respective national implementing legislations(as amended and replaced from time to time; the Swiss Federal Data Protection Act and its implementing ordinances (as amended and replaced from time to time); the Monaco Data Protection Act (as amended and replaced from time to time); the UK Data Protection Law (as amended and replaced from time to time) and any other data protection law of the European Union the European Economic Area (**EEA**) (together "**EU Data Protection Law**"); (2) the California Consumer Privacy Act of 2018 ("CCPA") as amended by the California Privacy Rights Act of 2020 and its implementing regulations ("CPRA"); (3) the Virginia Consumer Data Protection Act ("VCDPA"); (4) the Colorado Privacy Act ("CPA"); (5) the Connecticut Data Privacy Act ("CTDPA"); (6) the Utah Consumer Privacy Act ("UCPA"); (7) the U.S. Gramm-Leach-Bliley Act; (8) the Brazil General Data Protection Act; (9) the South Africa Protection of Personal Information Act; (10) the Personal Information Protection Law of the PRC and other PRC Laws relating to privacy and protection of Personal Information; (11) Argentina Personal Data Protection Act; (12) Kingdom of Saudi Arabia Personal Data Protection Law (amended 2023) and its Implementing Regulations; (13) Nigeria Data Protection Act 2023 and its subsidiary regulations and guidelines; (14) Turkey Law on the Protection Of Personal Data (DPL) No. 6698 and its regulations and successors; (15) Canadian federal and provincial laws governing the processing of Personal Information, (16) including the Personal Information Protection and Electronic Documents Act and substantially similar provincial laws; 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, national, provincial, and local requirements, in each case, as updated, amended or replaced from time to time

"**Process**" or "**Processing**" or "**Processing of Personal Data**" 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 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 or as defined under the applicable Privacy and Data Protection Law.

"**Sensitive Data**" (**or "Sensitive Personal Data," or "Sensitive Personal Information**"), which may be used interchangeably in this Agreement) means any Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation, as well as any other type of data that will be considered to be sensitive according to any Privacy and Data Protection Law as applicable.

"**Sub-Processor**" means the person (whether a natural person, a legal entity or any other organization) engaged by Supplier or any further sub-contractor to Process Personal Data on behalf of and under the instructions of Mastercard.

"**UK Data Protection Law**" means (i) the Data Protection Act 2018; (ii) the means the UK General Data Protection Regulation, amended by the UK Data Protection Act 2018, and as it may be amended from time to time 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.

"UK Standard Contractual Clauses" or **"UK SCCs"** means the UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, issued under Section 119A of the Data Protection Act 2018 by the Information Commissioner and laid before Parliament on 2 February 2022 in force 21 March 2022.

"**EU SCCs**" means in respect of Personal Data to which the EU GDPR was applicable prior to its processing by Supplier as Processor, the standard contractual clauses for the transfer of personal data to third countries adopted by the European

Commission under Commission Implementing Decision (EU) 2021/914 including the text from the modules of such clauses as specified in this Data Processing Agreement.

The terms "**Controller**," "**Data Subject**", "**Processor**", and "**Supervisory Authority**" shall have the meanings given to them under EU Data Protection Law.

3. **General Privacy and Data Protection.**

3.1. **Scope**.

All the obligations in this Data Processing Agreement apply to each Party without regard to the residency or location (permanent or otherwise) of any individual to whom any Personal Data relates, the location of a Party's operations, the extent to which it has targeted a particular geographic regions or jurisdictions, or any other factors.

3.2. **Compliance with Privacy and Data Protection Law.**

Both Parties represent and warrant that they will comply with Privacy and Data Protection Law when Processing Personal Data in the context of the Services, and that they will perform their obligations under this Data Processing Agreement in compliance with Privacy and Data Protection Law and, particularly: (i) that they will provide the level of privacy protection required by Privacy and Data Protection Law, and (i) where applicable, further represents and warrants that it understands and will comply with this Data Processing Agreement.

3.3. **Roles of the Parties**.

The Parties agree that Mastercard is a Business and/or Controller (or similar status that determines the purposes and means of Processing under applicable Privacy and Data Protection Law) or Processor acting on behalf of Mastercard's customers who act as Controllers of Personal Data Processed under this Data Processing Agreement, and Supplier is a Service Provider and/or Processor (or other similar status acting on behalf of Mastercard under applicable Privacy and Data Protection Law), and/or as Sub-Processor of Mastercard's customers for the Processing of Personal Data for the purpose of providing the Services specified in the Agreement and as implemented by each individual Statement of Work where applicable. Supplier must only Process Personal Data on Mastercard's behalf and instructions, or of Mastercard's customers, for a Business Purpose as strictly necessary to provide the Services specified in the Agreement. Mastercard, or the customers on whose behalf Mastercard may act, have the sole and exclusive authority to determine the purposes and means of the Processing of Personal Data that are disclosed to Supplier. Supplier is prohibited from Processing Personal Data for any other purpose.

3.4. **Instructions**.

3.4.1 Mastercard's instructions are documented in Annex 1 of Addendum A1of the Agreement and any applicable SOW(s). Mastercard may issue additional instructions to Supplier as it deems necessary to comply with Privacy and Data Protection Law. Supplier must notify Mastercard (1) when any law or legal requirement prevents Supplier (a) from fulfilling its obligations under this Data Processing Agreement or Privacy and Data Protection Law, and (b) from complying with the instructions received from Mastercard or (2) if the Supplier determines it can no longer fulfil its obligations under this Agreement or Privacy and Data Protection Law. Upon receiving notice from Supplier, the Parties shall work together to come to a mutual agreement to implement an agreeable solution for the purpose of ensuring compliance. In the meantime, Mastercard may in part or in whole, as applicable, direct Supplier to take reasonable and appropriate steps to stop and remediate unauthorized Processing, including suspending the Processing of Personal Data by Supplier, until such event resulting in non-compliance has ceased or has been rectified. If Supplier fails to correct the non-compliance or Parties cannot come to a mutual solution to rectify the non-compliance, Mastercard is entitled to terminate any further Personal Data Processing and the Agreement, if doing so is required to comply with Privacy and Data Protection Law.

3.4.2 Except as expressly permitted by Privacy and Data Protection Law and where applicable, Supplier is prohibited from (i) Processing including retaining, using, or disclosing Personal Data outside of the direct business relationship between the Parties, and (ii) combining Personal Data with Personal Data obtained from, or on behalf of, sources other than Mastercard.

3.4.3 Where Mastercard discloses or makes available de-identified data to Supplier, Supplier is prohibited from attempting to re-identify said data.

3.5. **Supplier Obligations**. Supplier agrees and warrants that it will:

3.5.1 **Data Protection Officer** where required under Privacy and Data Protection Law, appoint a data protection officer or similar function who will oversee the Processing of Personal Data conducted on behalf of Mastercard.

3.5.2 **Internal Records:** maintain internal records of all Processing conducted on behalf of Mastercard, with at the minimum the categories of information required under applicable Privacy and Data Protection Law and provide them to Mastercard upon request.

3.5.3 **Marketing Communications, Cookies and Similar Technologies**: where applicable, comply with all opt-in and opt-out requirements for sending marketing communications, consult any opt-out registers where applicable and comply with legal requirements applicable to cookies and similar technologies.

3.5.4 **Notification Obligations:** immediately inform Mastercard, in writing, in relation to any Personal Data Processed in the context of the Services of: (i) any requests from individuals or Data Subjects to exercise their Data Protection Rights; (ii) any request or complaint received from Mastercard's customers, consumers, employees or any other individual or Data Subject; (iii) any question, complaint, investigation or other inquiries from regulators or Data Protection Authorities; and (iv) any public authority of whatever jurisdiction requesting disclosure of or information about the Personal Data that are Processed by Supplier. Supplier agrees and warrants that it will provide a copy of any such requests within 48 (forty-eight) hours (or a shorter period of time if required by Privacy and Data Protection Law) of receipt by email to privacyanddataprotection@mastercard.com and that it will respond to such requests only in accordance with Mastercard's prior written authorization

3.5.5 **Cooperation and Assistance:** cooperate with Mastercard to ensure compliance with Privacy and Data Protection Law, this Data Processing Agreement, and Mastercard's or Mastercard's customers' instructions, and to assist Mastercard in fulfilling its own obligations under Privacy and Data Protection Law and as applicable Mastercard's or Mastercard's customer's instructions, including complying with individuals' or Data Subjects' requests to exercise their Data Protection Rights; verifying the identity of the individual or Data Subject making a request; replying to inquiries or complaints from individuals or Data Subjects; replying to investigations and inquiries from competent Government Bodies or Supervisory Authorities; conducting data protection impact assessments and consultations and other interactions with competent Government Bodies or Supervisory Authorities. Where required by Mastercard, the Supplier shall submit the Personal Data it holds on the individual or Data Subject in a format agreed and within the timeframe agreed by Mastercard.

3.5.6 **Return and Deletion of Personal Data:** upon expiry or termination of the Agreement and/or relevant SOW, or if the Agreement or any relevant part of the Agreement authorizing Supplier to Process Personal Data has been revoked, rescinded, or held void, invalid or unenforceable, or as set forth within the relevant SOW, comply with Mastercard's request, and at Mastercard's sole option, securely delete existing copies of the Personal Data or return the same to Mastercard without retention of any hard or soft copies, unless applicable local law requires storage of the Personal Data, in which case Supplier will protect the confidentiality of the Personal Data, will not actively Process the Personal Data anymore, and will continue to comply with this Data Processing Agreement. Supplier will issue a certificate of deletion upon Mastercard's request.

3.6. **Security of the Processing, Confidentiality, and Personal Data Breach Notification**. Supplier agrees and warrants that:

3.6.1 it has implemented and maintains a comprehensive written information security program that complies with Privacy and Data Protection Law and Appendix 1 of the Controller to Processor terms of this Data Processing Agreement. Supplier's written information security program must include appropriate technical and organizational measures to ensure a level of security appropriate to the risk, which includes at the minimum the security measures listed in Appendix 1 of the Controller to Processor terms of this Data Processing Agreement and as appropriate: (a) the pseudonymization and encryption of Personal Data (including the encryption of Primary Account Number (PAN) in transit and in rest); (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services (including by appropriately maintaining and reviewing logs, performing periodic password renewal and applying multi-factor authentication, in accordance with the controls referenced in Appendix 1 of the Controller to Processor terms of this Data Processing Agreement); (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 Supplier's technical and organizational measures for ensuring the security of the Processing of Personal Data. In assessing the appropriate level of security, Supplier 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. Supplier's Information Security Program shall comply with the applicable Payment Card Industry Data Security Standards to the extent Supplier Processes payment card information (hereinafter defined as ("**Information Security Program**").

3.6.2 Supplier undertakes to notify Mastercard of any technical, operational, organizational or other change having a material impact on the security, confidentiality or protection of Personal Data, no less than 15 (fifteen) working days prior to implementing any such change. Supplier agrees to submit its Information Security Program to the Data Protection and Security Audit as defined under section 3.9 of this Data Processing Agreement.

3.6.3 Supplier must take steps to ensure that any person (whether an individual, a legal entity or any other organization) acting under its authority, including any Sub-Processor, who has access to Personal Data is only granted access to Personal Data on a need-to-know basis, is subject to a duly enforceable contractual or statutory confidentiality obligation, and only Processes Personal Data in accordance with this Data Processing Agreement and Mastercard's instructions.

3.6.4 Supplier will inform Mastercard of any Personal Data Breach or where there is a reasonable suspicion that a Personal Data Breach has occurred i) in writing to SOC@mastercard.com, TPRM@mastercard.com and the account manager or person they are doing business with inside of Mastercard, and; ii) by contacting the Mastercard Operations Command Center (OCC) in Mastercard at +1-636-722-3600 or 1-800-358-3060 (US toll-free number) and selecting the option to be directed to Mastercard's Security Operations Center without undue delay, and no later than 24 (twenty-four) hours (or a shorter period of time if required by Privacy and Data Protection Law) after having become aware of a Personal Data Breach or the reasonable suspicion of a Personal Data Breach. Such notice shall summarize in reasonable detail the effect on Mastercard, if known, of the Personal Data Breach, the corrective action taken and to be taken by Supplier and/or its Sub-Processor, and other information as required by Privacy and Data Protection Law. Supplier shall and shall cause its Sub-Processors (if any), to promptly take all necessary and advisable corrective actions and fully cooperate with Mastercard in all reasonable and lawful efforts to prevent, mitigate, investigate or rectify such Personal Data Breach, including in relation to any forensic investigation or related audit requested by Mastercard. Mastercard is free to use the forensic investigator of its choice. Supplier shall collect, preserve and document all evidence regarding the discovery and cause of, and vulnerabilities, response, remedial actions, and impact, related to the Personal Data Breach, and shall provide such documentation to Mastercard upon request. Supplier will be responsible for the costs and expenses associated with the performance of its and its Sub-Processor's obligations described in this paragraph, unless the Personal Data Breach is caused by the acts or omissions of Mastercard. Supplier will assist Mastercard in complying with its own obligations or with Mastercard's customers' obligations under Privacy and Data Protection Law to notify a Personal Data Breach. In case of conflict between this Section 3.6.4 and section 3.9, this section 3.6.4 will prevail.

3.6.5 Except to the extent prohibited by applicable legal, regulatory or law enforcement requirements, Supplier must obtain the written approval of Mastercard prior to the publication or communication of any filings, communications, notices, press releases or reports related to any Personal Data Breach that expressly mention Mastercard or its Affiliates. Supplier acknowledges and agrees that a violation of this section 3.6, or the occurrence of any Personal Data Breach, may cause immediate and irreparable harm to Mastercard for which money damages may not constitute an adequate remedy. Therefore, Supplier agrees that Mastercard may seek injunctive or other equitable relief for any such violation or incident, in addition to its remedies at law, without proof of actual damages.

3.6.6 Supplier agrees and warrants that it has not purposefully created back doors or similar programming that could be used to access the Personal Data in transit or at rest, or otherwise created business processes to facilitate mass and indiscriminate access to Personal Data by Government Agencies. Supplier must notify Mastercard by email to privacyanddataprotection@mastercard.com as soon as it becomes aware of the existence of a back door or similar programming or of a new business process which enables mass and indiscriminate access to Personal Data.

3.7. **International Data Transfers**

3.7.1 Supplier agrees and warrants that it will not transfer Personal Data or allow access to Personal Data from outside the jurisdictions as listed under Annex 1 of Addendum A1 of the Agreement or otherwise authorized by Mastercard in writing in advance under the respective Statement of Work. Any transfer shall only be made with prior explicit written consent of Mastercard.

3.7.2 If Supplier is authorized under the Agreement to transfer Personal Data, it must ensure that the Personal Data will be protected with the same level of protection as provided by this Data Processing Agreement and, where required, implement any data transfer mechanism required by Privacy and Data Protection Law.

3.7.3 Supplier represents and warrants that it is not subject to a requirement under applicable Law including Privacy and Data Protection Law that would prevent Supplier from transferring Personal Data in accordance with this Data Processing Agreement.

3.7.4 Supplier agrees that Mastercard may have supplementary Personal Data transfer and localization requirements arising from contractual obligations. In those cases, Mastercard will instruct Supplier under the applicable SOW, not to transfer the Personal Data out of the original jurisdiction and Supplier commits to not proceed with said Personal Data transfers.

3.7.5 **European Specific Provision**:

3.7.5.1 Supplier agrees and warrants that it is prohibited from transferring Personal Data outside of Europe except as listed above in section 3.7.1 and if it obtains the explicit written consent of Mastercard and provided that the Personal Data are transferred to a jurisdiction which has been considered to provide an adequate level of protection under EU Data Protection Law or to a data recipient which has implemented adequate safeguards under EU Data Protection Law such as approved Binding Corporate Rules or Standard Contractual Clauses. Supplier agrees to protect Personal Data in the jurisdictions listed in Section 3.7.1 of this Data Processing Agreement in compliance with EU Data Protection Law, and this Data Processing Agreement and will not use the Personal Data transferred to the jurisdictions listed in Section 3.7.1 of this Data Processing Agreement for its own purposes.

3.7.5.2 Where Supplier transfers Personal Data subject to the EU GDPR or the UK GDPR to a country that is not subject to a European Commission adequacy decision; or transfers Personal Data subject to the Swiss Data Protection Law to a country that is not considered to provide for adequate data protection legislation by the Federal Council ("**EU/Swiss Transfers**"), the Parties agree that the transfer shall be governed by the SCCs, which are hereby incorporated into this Agreement by reference, subject to section 3.7.5.3 of this Agreement. The Parties agree that signature to and dating of this Agreement shall constitute all required signatures and dates for the SCCs.

3.7.5.3 For the purposes of the EU SCCs that apply pursuant to section 3.7.5.2 of this Data Processing Agreement, the Parties agree the following:

a) the text from module two of the EU SCCs shall apply where Mastercard is the Controller, the text from module three of the EU SCCs shall apply where Mastercard is a Processor on behalf its customers and no other modules or any clauses marked as optional in the EU SCCs shall apply;

b) for the purposes of clause 9(a) of the EU SCCs, as applicable under modules two and three, option 1 applies with 60 business days as the specified time period for submitting the request for specific authorization. Any request pursuant to clause 9(a) of the EU SCCs shall be made pursuant to section 3.8.7 of this Data Processing Agreement, including the information required thereof, which shall be provided in addition to any other information necessary to enable Mastercard to decide on the authorization. The list of Sub-processors already authorized by Mastercard required by Annex III of the EU SCCs is set out in Annex 1 of Addendum A1 of the Agreement or otherwise authorized by Mastercard in writing in advance under the respective SOWs;

c) the information as required by Annex I of the EU SCCs is as set out in Annex 2 of Addendum A1of the Agreement and the signatures for the purpose of Annex I of the EU SCCs are the signatures to the Agreement and the date is the date of the Agreement;

d) the technical and organisational measures required by Annex II of the EU SCCs are as set out in Appendix 1 of the Controller to Processor terms of this Data Processing Agreement and Annex 2 of Addendum A1 of the Agreement and the information in relation to the technical and organisational measures in relation to Data Subject rights as required by clause 10(b) and Annex II of the EU SCCs as applicable under modules two and three are as set out in Annex 2 of Addendum A1 of the Agreement;

e) any notice provided under clause 9(d) of the EU SCCs shall be provided according to the timing and to the email address as set out in section 3.8.8 of this Data Processing Agreement;

f) any notice provided under clause 14(e) or clause 16 of the EU SCCs shall be provided according to the timing and to the email address as set out in section 3.7.9 of this Data Processing Agreement;

g) for the purposes of clause 17 of the EU SCCs, option 1 applies and the EU SCCs shall be governed by the laws of Belgium and for the purposes of clause 18 of the EU SCCs, the courts of Belgium shall have jurisdiction in relation to the EU SCCs; and

h) notwithstanding anything contrary in this Data Processing Agreement or the Agreement, clause 5 of the EU SCCs shall apply and, as such, in the event of a contradiction between the EU SCCs and the provisions of this Data Protection Agreement or the Agreement, the EU SCCs shall prevail.

3.7.5.4 Applicable Law and Jurisdiction:

The Processing of Personal Data subject to EU Data Protection Law under this Exhibit is governed by Belgian law and any disputes between the Parties relating to the Processing of Personal Data subject to EU Data Protection Law will be subject to the exclusive jurisdiction of the courts in Belgium, expect for section 3.7.7 of this Data Processing Agreement in which case laws of England and Wales apply and any dispute arising from it shall be resolved by the courts of England and Wales and section 3.7.6 in which case the ordinary courts of Zurich, canton of Zurich, Switzerland.

3.7.6 **Swiss Specific Provision:**

In respect of Personal Data to which Swiss Data Protection Law applies, (i) in deviation of clause 13 (a) of the EU SCCs in connection with its Annex I.C., the competent supervisory authority in Annex I.C. shall be the Swiss Federal Data Protection and Information Commissioner and all references to the "competent supervisory authority" shall be interpreted accordingly; (ii) in deviation of clause 17 of the EU SCCs, the EU SCCs shall be governed by and construed in accordance with the substantive laws of Switzerland; (iii) in deviation of clause 18 (a) and (b) of the EU SCCs, any disputes arising from the EU SCCs shall be subject to the exclusive jurisdiction of the ordinary courts of Zurich, canton of Zurich, Switzerland; (iv) any references to "Regulation (EU) 2016/679" and specific articles thereof in the EU SCCs should be interpreted to refer to Swiss Data Protection Law and its corresponding provisions, as applicable; (v) in supplementation of clause 8.7 of the SCCs, 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 (vi) the term "member state" shall 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) and clause 18(c) of the EU SCCs shall be interpreted accordingly.

3.7.7 **UK Specific Provision**:

To the extent a Supplier receives any Personal Data subject to the UK GDPR from Mastercard and Processes or transfers such Personal Data in a country that is not subject to a UK government adequacy decision ("**UK Transfers**"), the Supplier agrees that such UK Transfers shall be governed by standard data protection clauses issued by the UK Information Commissioner under S119A(1) Data Protection Act 2018 ("UK Addendum"), which is hereby incorporated into this Data Processing Agreement by reference, but as permitted by clause 17 of such UK Addendum, the parties agree to change the format of the information set out in Part 1 of the UK Addendum so that: (i) the details of the parties as set out in Table 1, and their signatures are included in the Annex 2 of the Addendum A1 of the Agreement; (ii) in Table 2, the first option is selected and the "Approved EU SCCs" are those incorporated into this Data Processing Agreement as per section 3.7.5.3; (iii) in Table 3, "Annex 1A and 1B to the Approved EU SCCs" are Annex 2 of Addendum A1 of the Agreement, "Annex II to the Approved EU SCCs" are Appendix 1 of the Controller to Processor terms of this Data Processing Agreement and "Annex III to the Approved EU SCCs" are Annex 1 of Addendum A1of the Agreement or as listed under the applicable SOWs; and (iv) in Table 4, Neither Party shall have the right to end this Addendum pursuant to Section 19. The UK Transfers shall be governed by the laws of England and Wales and any dispute arising from it shall be resolved by the courts of England and Wales. The Parties agree, that Mastercard may make any amendments to the application of the EU SCCs, the application of the UK Addendum and/or any other amendments to this section 3.7.7 of this Data Processing Agreement in respect of UK transfers as it deems necessary to implement any replacement standard contractual clauses approved for use under Article 46 of the UK GDPR.

3.7.8 For the purpose of Processing of Personal Data subject to EU Data Protection Law, Supplier will notify Mastercard in writing to TPRM@mastercard.com, with the subject line "Europe Data Processing Addendum Notification", at least 60 calendar days prior to any new intended data transfer to a country that is not subject to a European Commission adequacy decision, or deemed a country not providing for adequate data protection legislation by the Federal Council, as applicable including the justification of the necessity of the transfer, an explanation of any adequate supplementary measures implemented by the Supplier to ensure essential equivalence if necessary or justified and an explanation if Supplier considers that such safeguards are not necessary. Any such transfer is subject to Mastercard's prior written consent. Where Mastercard does not consent to such transfer and further Processing of Personal Data is not possible without such transfer, Mastercard may in part or as a whole, as applicable, suspend the Processing of Personal Data by Supplier or terminate the Agreement, whichever is appropriate.

3.7.9 For the purpose of Processing of Personal Data subject to EU Data Protection Law, Supplier will promptly and no later than 48 hours from becoming aware inform Mastercard in writing to TPRM@mastercard.com, with the subject line "Europe Data Processing Addendum Notification", if (1) it has reason to believe that it is or has become subject to laws or practices that prevent the Supplier from fulfilling its obligations under the EU SCCs , and (2) it is unable to comply with the EU SCCs , for whatever reason. Supplier shall provide the description of the non-compliance and the reasons for the non-compliance, and its impact or likely impact on Mastercard or Mastercard customers.

3.8. **Data Provision or Disclosure to Sub-Processors**

3.8.1 Supplier must not share, transfer, transmit, disclose or otherwise provide access to or make available any Personal Data to any person (whether a natural person, legal entity or any other organization) other than those Sub-Processors listed under Annex 1 of Addendum A1of the Agreement or otherwise authorized by Mastercard in writing in advance under the respective SOWs.

3.8.2 Without prejudice to Section 3.8.1 above, Supplier must ensure that, in each instance in which it engages a Sub-Processor to Process Personal Data on Mastercard's behalf it must enter into a binding written agreement with the Sub-Processor with the same security and privacy and data protection obligations that apply to Supplier under this Data Processing Agreement and Privacy and Data Protection Law.

3.8.3 Prior to any sub-processing, Supplier must carry out adequate due diligence to ensure that the Sub-Processor is capable of (i) Processing Personal Data with at least the same level of protection for the Processing of Personal Data and of (ii) complying with the same security and privacy and data protection obligations as are imposed on Supplier under this Data Processing Agreement and Privacy and Data Protection Law.

3.8.4 Supplier must inform Mastercard in writing at least 60 calendar days prior to any change to the role or status of the Sub-Processor. Mastercard may object in writing to Supplier's appointment of a new Sub-Processor on reasonable grounds by notifying Supplier in writing within 30 calendar days of receipt of notice in accordance with this section. In the event Mastercard objects, the Parties shall discuss Mastercard's concerns in good faith with a view to achieving a commercially reasonable resolution.

3.8.5 Supplier will provide Mastercard with the necessary information to help verifying the Sub-Processor's compliance with its data protection obligations (including, where appropriate, attestations and certifications of the Sub-Processor's compliance with data protection and information security standards, such as the Payment Card Industry Data Security Standards (PCI-DSS) and ISO certifications, as applicable).

3.8.6 Supplier will remain fully liable towards Mastercard for the performance by each Sub-Processor of any and all Sub-Processor's obligations under the agreement between Supplier and such Sub-Processor and any other act or omission by such Sub-Processor in relation to the Processing of Personal Data thereunder.

3.8.7 Supplier will notify Mastercard in writing to TPRM@mastercard.com, with the subject line "Europe Data Processing Addendum Notification", about engaging any intended new Sub-Processor(s) or subsequent Sub-Processor(s) with at least 60 business days notice prior to the engagement of the Sub-processor and such notice shall include the description of the Processing by each such Sub-Processor, categories of Data Subjects and the categories of Personal Data Processed, and the location of the Processing of Personal Data. Where Mastercard does not consent to the intended new Sub-Processor(s) or subsequent Sub-Processor(s) and the Processing of Personal Data is not possible without the involvement of the particular Sub-Processor(s) or subsequent Sub-Processors(s) that was objected to by Mastercard, Mastercard may in part or as a whole, as applicable, suspend the Processing of Personal Data by Supplier or terminate the Agreement, whichever is appropriate.

3.8.8 Supplier will promptly and no later than 48 hours from becoming aware notify Mastercard, in writing to TPRM@mastercard.com, with the subject line "Europe Data Processing Addendum Notification", of any failure by Supplier or any Sub-Processor(s) or subsequent Sub-Processor(s) to fulfil its obligations under this Data Processing Agreement or sub-agreement, including but not limited to where Supplier has engaged any new Sub-Processors, or where Personal Data has been transferred to any new locations, without Mastercard's prior written consent.

3.9. **Data Protection and Data Security Audit**

3.9.1 Upon request by Mastercard and subject to Mastercard's reasonable discretion, Supplier allows Mastercard or, as applicable, Mastercard's customers, or an inspection body composed of independent members selected by Mastercard or Mastercard's customers, to audit and review Supplier's Information Security Program, data processing facilities, and data protection compliance program to verify compliance with this Data Processing Agreement, Privacy and Data Protection Law, and as applicable, Mastercard's customers' instructions or own obligations. Where a Personal Data Breach was caused by a Sub-

Processor engaged by Supplier, Supplier undertakes to ensure that such Sub-Processor fully cooperates with Mastercard, and where requested by Mastercard, allows Mastercard to audit and review such Sub-Processor's Information Security Program, data processing facilities, and data protection compliance program. ("hereinafter defined as "**Data Protection and Security Audit**").

3.9.2 The Parties will mutually agree upon the scope, timing, and duration of the Data Protection and Security Audit. The Data Protection and Security Audit may be conducted by an independent third-party auditor designated by Mastercard, in which case Supplier will make available to Mastercard, or where applicable Mastercard's customer, the result of the Data Protection and Security Audit.

3.9.3 Supplier agrees to fully cooperate with such Data Protection and Security Audit and implement all commercially reasonable changes to its Information Security Program, data processing facilities and data protection compliance program that, as a result of the Data Protection and Security Audit, are required to ensure Supplier's compliance with this Agreement, Privacy and Data Protection Law, and as applicable, Mastercard's customer's instructions or own obligations. Supplier's failure to allow or cooperate with any Data Protection and Security Audit or implement any required changes to its Information Security Program, data Processing facilities or data protection compliance program shall entitle Mastercard to suspend the Processing of Personal Data by Supplier, and to terminate any further Personal Data Processing and terminate the Agreement, if doing so is reasonably required or expected by Mastercard to comply with this Data Processing Agreement, Privacy and Data Protection Law, and as applicable, Mastercard's customers' instructions or own obligations.

3.9.4 Upon request by Mastercard, Supplier must provide a certification of compliance with applicable Privacy and Data Protection Law and information security standards, such as the Payment Card Industry Data Security Standards (PCI-DSS) and SOC2 and ISO certifications, as applicable.

3.10. **Liability**. The Parties agree that:

3.10.1 Supplier is fully liable to Mastercard for any violations or breaches of Privacy and Data Protection Law or of this Data Processing Agreement by Supplier or any of its Sub-Processors. For the avoidance of doubt, any exclusion or limitation of liability provided in the Agreement will not apply to Supplier's liability for infringements of Privacy and Data Protection Law or this Data Processing Agreement.

3.10.2 If Mastercard has paid, has been imposed an obligation to pay, or has otherwise been held liable for payment of any compensation, damages or fines to any individual, competent Government Body or other third party due to any violations or breaches by Supplier or any of its Sub-Processors, Mastercard is entitled to claim back from Supplier that part of the compensation, damages or fines, corresponding to Supplier's part of responsibility for the compensation, damages or fines.

3.11. **Parties to Data Processing Agreement.**

Where the Processing of Personal Data is subject to EU Data Protection Law or where EU SCCs apply, Mastercard Europe S.A. is the signatory to this Exhibit and the EU SCCs.

3.12. **Change in Law**

Mastercard will make an amendment to this Data Processing Agreement as are reasonably necessary from time to time to update and address the requirements of Privacy and Data Protection Law.

Appendix 1: SECURITY MEASURES

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

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Supplier will, as a minimum, implement the security measures listed in "Security Requirements for Suppliers and Business Partners" at https://procurement.mastercard.com/information_suppliers.html, as may be updated from time to time. These security measures must be implemented in addition to any standards, certifications or audit requirements that Supplier adheres to (or has been certified to) with regard to the Services or Deliverables, including but not limited to the Payment Card Industry Data Security Standards (PCI-DSS) and ISO certifications, as applicable.

Appendix 2: Region Specific Privacy Terms

A. **China Data Processing Addendum**. The Parties agree that they will amend and supplement the terms as provided by Mastercard for the purposes of compliance with Privacy and Data Protection Law of the PRC if there is cross border transfer of Personal Data subject to the Privacy and Data Protection Law of the People's Republic of China ("China" or the "PRC", for the purposes of this Agreement, exclusive of Hong Kong Special Administrative Region, Macau Special Administrative Region and Taiwan).

B. **Japan Data Processing Addendum.** The Parties agree that they will amend and supplement the terms as provided by Mastercard for the purposes of compliance with Privacy and Data Protection Law of Japan in the event where (i) Mastercard conducts, in Japan, Processing of Personal Data of data subjects located in or out of Japan, and Supplier conducts in or out of Japan Processing of the said Personal Data on behalf of Mastercard or Mastercard's customers pursuant to this Agreement, or (ii) Supplier Processes, in or out of Japan, Personal Data of data subjects located in Japan pursuant to this Agreement.

C. **CCPA.**

1. Additional Definitions.

a. "CCPA" means the California Consumer Privacy Act of 2018, as amended, including as amended by the California Privacy Rights Act of 2020, together with all implementing regulations.

b. The terms "business", "business purpose", "consumer", "personal information", "processing", "sale", "sell", "service provider", and "share" have the meanings given in the CCPA.

2. **Prohibitions**. Without prejudice to Supplier's obligations under Section 3.4, with respect to the processing of Personal Data in accordance with the CCPA, Supplier will not, unless otherwise permitted under the CCPA:

a. Sell or where applicable, Share any Personal Data and any data derived or inferred from Personal Data or from Processing Personal Data to develop or promote competing services;

b. retain, use or disclose Personal Data:

i. other than for a business purpose under the CCPA or on behalf of Mastercard and for the specific purpose of performing the Services as defined under the Agreement.
ii. outside of the direct business relationship between the Parties; or

c. combine Personal Data with Personal Data obtained from, or on behalf of, sources other than Mastercard.

3. **Compliance**. (i) Supplier will provide the level of privacy protection required by CCPA, and (ii) where applicable, further represents and warrants that it understands and will comply with this Data Processing Agreement. Supplier will Process Personal Data in compliance with this Data Processing Agreement and CCPA. Supplier will notify Mastercard if, Supplier is unable to meet its obligations under the CCPA and this Data Processing Agreement.

D. **Argentina.**

1 If the Processing of Personal Data of Data Subjects is subject to the Argentina Personal Data Protection Act 25.326 (PDPA) (Ley de Protección de los Datos Personales) is involved, Supplier agrees to comply with the obligations of a data importer as set out in the model contract titled Contrato Modelo de Transferencia Internacional de Datos Personales con Motivo de Prestación de Servicios adopted by the Data Protection Agency of the Republic of Argentina under Disposition 60 — E/2016 (the 'Argentinian SCCs') for the transfer of personal data to data processors established in third countries.

a) Supplier acknowledges that each Data Exporter in the Republic of Argentina will be a Data Controller as defined in the PDPA. In particular, and without limiting the above obligation:

(i) Supplier agrees to grant third party beneficiary rights to data subjects, as set out in Clause 3 of the Argentinian SCCs, provided that Supplier's liability shall be limited to its own processing operations; and

(ii) Supplier agrees that its obligations under the Argentinian SCCs shall be governed by the laws of the Republic of Argentina in which the Data Exporter(s) are established; and

(iii) the details of the appendices applicable to the Argentinian SCCs are set out in Annex 1 of Addendum A1 of the Agreement or under the applicable SOWs insofar as it relates to Data Processor purposes.

b) For the purposes of Annex A to the Argentinian SCCs, the data exporter is a Mastercard entity; the data importer is [Supplier name] and details about the data subjects, categories of data, processing operations and security measures are as set out in Annex 1 of Addendum A1of the Agreement or the applicable SOWs and Appendix 1 of this Data Processing Agreement for security measures.

2 If the Processing of Personal Data of Data Subjects is subject to the Argentina Personal Data Protection Act 25.326 (PDPA) (Ley de Protección de los Datos Personales), Supplier shall neither apply nor use the Exported Personal Information , as defined under the Argentina Personal Data Protection Act for any purpose other than the [ones specified as 'Processor' purposes in Annex 1 of Addendum A1 of the Agreement] nor shall the Supplier, except as permitted in this Data Processing Agreement, communicate to other parties such Exported Personal Information, even for storage purposes. Once the corresponding contractual obligations have been performed, the Exported Personal Information processed must be destroyed, except where there is an express authorization given by the person for account of whom such services are rendered, by reason of a possibility of the exported Personal Information being used for future services, in which case the exported Personal Information may be stored under due security conditions for a maximum term of up to two years. The Parties agree to adopt confidentiality measures to protect the exported Personal Information following only instructions from the Data Controller as defined in the section 9 of PDPA. Supplier shall process the exported Personal Information following only instructions from the Data Controller.

.

CONTROLLER TO CONTROLLER SPECIFIC TERMS AND CONDITIONS

1. Privacy and Data Protection. This Data Processing Agreement ("**Data Processing Agreement**") supplements the Master Supplier Agreement (the "**Agreement**") between Mastercard and Supplier and governs the Processing of Personal Data subject to Privacy and Data Protection Law for the Services provided in this Agreement. If Supplier or any Supplier Personnel receives, has access to or otherwise Processes Personal Data, Supplier shall comply with the requirements of the Data Processing Agreement. This Data Processing Agreement is intended to satisfy legal requirements under Privacy and Data Protection Law.

2. The terms used in this Data Processing Agreement have the meaning set forth herein. Capitalized terms not otherwise defined herein have the meaning given to them in the Agreement. Except as modified below, the terms of the Agreement remain in full force and effect. Addendum A2, Appendix 1 and Appendix 2 form an integral part of this Data Processing Agreement.

3. Definitions. In this Data Processing Agreement, the following definitions apply:

3.1. The terms "**Controller**," "**Data Subject**," "**Processor**" and "**Supervisory Authority**" shall have the meanings given to them under European Data Protection Law.

3.2. "**Business Purpose**" (or "**Purpose**") means the use of Personal Data for Mastercard or Supplier's operational purposes, or other notified purposes, provided that the use of Personal Data is reasonably necessary and proportionate to achieve the operational purpose for which the Personal Data was collected or processed or for another operational purpose that is compatible with the context in which the Personal Data was collected.

3.3. "**Data Protection Rights**" means all rights granted to individuals under applicable Privacy and Data Protection Law, which may include the right to know, the right of access, reproduction, supplement, rectification, or erasure to or of Personal Data, the right to raise complaints, the rights relating to data portability, restriction on Processing, and objection to the Processing (including the right to withdraw consent); and the rights relating to automated decision-making and indemnification against misuse of Personal Data.

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

3.5. "**Europe"** means the EEA, Switzerland, Monaco and the United Kingdom.

3.6. "**EU Personal Data**" means the processing of personal data to which data protection legislation of the European Union, or of a Member State of the European Union or European Economic Area, was applicable prior to its processing by the Supplier or Mastercard.

3.7. "**European Data Protection Law**" means the GDPR, the UK GDPR 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 respective national implementing legislations (as amended and replaced from time to time); the Swiss Federal Data Protection Act and its implementing ordinances ("**FADP**") (as amended and replaced from time to time); the Monaco Data Protection Act (as amended and replaced from time to time); the UK Data Protection Law, as defined in Section 1.11 below (as amended and replaced from time to time); and any other data protection law of the European Union, the European Economic Area ("**EEA**") or their respective member states, Switzerland, Monaco and the United Kingdom (as amended and replaced from time to time).

3.8. **"EU Standard Contractual Clauses"** or **"SCCs"** means: in respect of the EU Personal Data, the standard contractual clauses for the transfer of personal data to third countries pursuant to GDPR, adopted by the European Commission under Commission Implementing Decision (EU) 2021/914 including the text from the modules of such clauses as specified in this Agreement; and in respect of Swiss Personal Data, the same, as adapted to satisfy Swiss law requirements as specified in Section 6.1.1.8 of this Data Processing Agreement.

3.9. **"Existing Agreement"** means any written agreement or data processing agreement, or any other relevant agreement entered into by Mastercard and Supplier which involve Processing of Personal Data subject to EU GDPR and/or UK GDPR and/or FADP in the context of the Services.

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

3.11. **"Mastercard Binding Corporate Rules"** (or "**Mastercard BCRs**") means the Mastercard Binding Corporate Rules as approved by the data protection authorities, available at: https://www.mastercard.us/content/dam/mccom/global/documents/mastercard-bcrs.pdf;

3.12. "**Personal Data**" or "**Personal Information**" (which may be used interchangeably in this Agreement) means any information relating to an identified or identifiable individual, whether directly or indirectly identifiable, including but not limited to contact information, demographic information, passport number, Social Security number or other national identification number, bank account information, Primary Account Number, and authentication information (e.g., identification codes, passwords).

3.13. "**Personal Data Breach"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, access to, or other unauthorized Processing of Personal Data transmitted, stored or otherwise Processed.

3.14. "**Privacy and Data Protection Law**" means any Law, statute, declaration, decree, legislation, enactment, order, ordinance, regulation, rule, circular (as amended and replaced from time to time) which relates to the protection of individuals with regards to the Processing of Personal Data to which the Parties are subject, including but not limited to the GDPR, 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 respective national implementing legislations; the Swiss Federal Data Protection Act and its implementing ordinances ("**FADP**"); the Monaco Data Protection Act; the UK General Data Protection Regulation; and any other data protection law of the European Union, the European Economic Area ("**EEA**") or their respective member states, Switzerland, Monaco and the United Kingdom, all as amended and replaced from time to time. The definition includes also the California Consumer Privacy Act of 2018 (California Civil Code §§ 1798.100 to 1798.199) and its implementing regulations ("**CCPA**"), as amended including by the California Privacy Rights Act ("**CPRA**"); the U.S. Gramm-Leach-Bliley Act; the Brazil General Data Protection Act; the South Africa Protection of Personal Information Act; the Personal Information Protection Law of the PRC and other PRC Laws relating to privacy and protection of Personal information; Kingdom of Saudi Arabia Personal Data Protection Law (amended 2023) and its Implementing Regulations; Nigeria Data Protection Act 2023 and its subsidiary regulations and guidelines, Turkeye Law on the Protection Of Personal Data (DPL) No. 6698 and its regulations and successors; Canadian federal and provincial laws governing the processing of Personal Information, including the Personal Information Protection and Electronic Documents Act and substantially similar provincial laws; 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, national, provincial, and local requirements; each as applicable.

3.15. "**Process**" or "**Processing**" or "**Processing of Personal Data**" 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 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 or as defined under the applicable Privacy and Data Protection Law.

3.16. "**Sell**" means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's Personal Data by the business to another business or a third party for monetary or other valuable consideration.

3.17. "**Sensitive Data**" (or "**Sensitive Personal Data**," which may be used interchangeably in this Agreement) means any Personal Data considered to be sensitive according to applicable Privacy and Data Protection Law and may include data revealing racial or ethnic origin, political opinions, cult, religious or philosophical beliefs, or trade union membership, criminal records, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation, as well as any other type of data that will be considered to be sensitive according to any Privacy and Data Protection Law.

3.18. "**Sub-Processor**" means the entity engaged by a Party or any further sub-contractor to Process Personal Data on behalf of and under the instructions of such Party.

3.19. "**Swiss Personal Data**" means personal data to which FADP was applicable prior to its processing by the Supplier or Mastercard.

3.20. "**UK Addendum**" means the International Data Transfer Addendum to the EU 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);

3.21. **"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, as relevant; and (iii) the e-Privacy Directive 2002/58/EC (as amended by Directive 2009/136/EC) as transposed into UK national law.

3.22. **"UK GDPR"** means the UK General Data Protection Regulation, as amended by the UK Data Protection Act, and as it may be amended from time to time.

3.23. "**UK Standard Contractual Clauses**" or "**UK SCCs**" means the UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, issued under Section 119A of the Data Protection Act 2018 by the Information Commissioner and laid before Parliament on 2 February 2022 in force 21 March 2022.

4. General Privacy and Data Protection.

4.1. **Scope**. The Parties will comply with their respective obligations as set forth in this Agreement without regard to the residency or location (permanent or otherwise) of any individual to whom any Personal Data relates, the location of a Party's operations, the extent to which it has targeted particular geographic regions or jurisdictions, or any other factors.

4.2. **Compliance with Privacy and Data Protection Law**. Both Parties represent and warrant that they will comply with Privacy and Data Protection Law when Processing Personal Data in the context of the Services, and that they will perform their obligations under this Agreement in compliance with Privacy and Data Protection Law.

4.3. **Roles of the Parties**. The Parties acknowledge and confirm that each Party is responsible for the Processing of Personal Data for its own Business Purposes (as specified in Annex 1 of Addendum A2 of the Agreement or respective SOW) in the context of the Services specified in the Agreement. Each Party has the sole and exclusive authority to determine the Business Purposes and means of the Processing of Personal Data. The Parties acknowledge and confirm that each Party is a Business or, under European Data Protection Law, a Controller, for the Processing of Personal Data for its own Business Purposes in the context of the Services. The Parties further confirm that neither Party acts as a Service Provider nor, under European Data Protection Law, a Processor on behalf of the other Party; and that each Party is an independent Controller; and that the Agreement does not create a joint-Controllership or a Controller-Processor relationship between the Parties. Supplier warrants that it will not a) any Personal Data that is disclosed to it under this Agreement or any data derived or inferred from such Personal Data; or (b) Process such Personal Data to develop or promote competing services.

4.4. **Obligations of the Parties.** Each Party represents and warrants that, in relation to the Processing of Personal Data for its own Business Purposes in the context of the Services, that it will:

4.4.1. **Notice and Consent.** rely on a valid legal ground under Privacy and Data Protection Law for each of its own Business Purposes in the context of the Services, including provide appropriate notice to and/or seek consents from Data Subjects as required or appropriate under Privacy and Data Protection Law.

4.4.2. **Transfers.** ensure that, for any transfers of Personal Data in the context of the Services, the Personal Data will be protected with the same level of protection as provided under the Privacy and Data Protection Laws and this Agreement and it will implement any data transfer mechanism as required under Privacy and Data Protection Law.

4.4.3. **Data Subject Rights.** put in place a mechanism to allow a Data Subject to exercise their rights relative to their Personal Data under applicable Privacy and Data Protection Law.

4.4.4. **Cooperation and Assistance.** cooperate with the other Party in good faith to fulfil their respective data protection compliance obligations under Privacy and Data Protection Law, including complying with individuals' requests to exercise their Data Protection Rights and replying to investigations and inquiries from competent Government Bodies.

4.4.5. **Data Retention.** retain Personal Data until such time, 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.

4.4.6. **Termination.** upon termination of the Agreement and/or relevant SOW, or as set forth within the relevant SOW, comply with Mastercard's request, and securely delete existing copies of the Personal Data unless applicable local Law requires storage of the Personal Data, in which case Supplier will protect the confidentiality of the Personal Data, will not actively Process the Personal Data anymore, and will continue to comply with this Agreement.

4.5. Additionally, when processing EU Personal Data, each Party represents and warrants that, in relation to the Processing of said Personal Data for its own Purposes in the context of the Services, it acts as a Controller and that it:

4.5.1. complies with European Data Protection Law in respect of Processing of Personal Data (lawfulness of processing);

4.5.2. relies on a valid legal ground, as required, under European Data Protection Law for each of its own Purposes, including obtaining Data Subjects' appropriate consent if required or appropriate under European Data Protection Law (legal ground);

4.5.3. provides appropriate notice to the Data Subjects regarding (1) the Processing of Personal Data for its own Purposes, in a timely manner and at the minimum with the elements required under European Data Protection Law, (2), as appropriate, the existence of Mastercard BCRs (notice);

4.5.4. 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 (accuracy, data minimization and data retention);

4.5.5. 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 European Data Protection Law (accountability);

4.5.6. responds to Data Subject requests to exercise their rights granted to individuals under European Data Protection Law, including but not limited to the right of (a) access, (b) rectification, (c) erasure, (d) data portability, (e) restriction of Processing, and (f) objection to the Processing in accordance with European Data Protection Law (data subjects' rights);

4.5.7. Cooperates with the other Party to fulfil their respective data protection compliance obligations under European Data Protection Law (cooperation); and

4.5.8. has not purposefully created back doors or similar programming that could be used to access the Personal Data in transit or at rest, or otherwise created business processes to facilitate mass and indiscriminate access to Personal Data by Government Agencies ("**government data request**")

4.6. **Notification Obligations.** Supplier agrees and warrants that it will immediately inform Mastercard, in writing of any request, question, objection, complaint, investigation or any other inquiry, received from any individual, regulator, public authority or other Government Body of whatever jurisdiction or other Government Body, that relates to Personal Data Processed by Mastercard in the context of the Services, unless otherwise restricted by applicable Law. Supplier will provide a copy of any such requests within 48 (forty eight) hours (or a shorter period of time if required by Privacy and Data Protection Law) of receipt by email to privacyanddataprotection@mastercard.com and will respond to such requests only in accordance with Mastercard's prior written authorization, unless otherwise prohibited by applicable Privacy and Data Protection Law.

4.7. **Accountability.** Supplier agrees and warrants that it will implement appropriate administrative, technical, operational and organizational measures to ensure, and to be able to demonstrate, that the Processing of Personal Data is performed in accordance with this Agreement and applicable Privacy and Data Protection Law.

4.8. Where Mastercard discloses or makes available de-identified data to Supplier, Supplier represents and warrants it will not attempt to re-identify said data.

5. Data Disclosures.

5.1.1. The Parties represent and warrant that they will only disclose Personal Data Processed to a third party in the context of the Services in accordance with Privacy and Data Protection Law and with this Agreement and will require such third party in writing to comply with Privacy and Data Protection Law and with the same privacy and data protection obligations as are imposed on the disclosing Party by this Agreement, as appropriate and relevant, unless it is not possible to do so, such as where the data recipient is a Governmental Body.

6. Data Transfers. Each Party represents and warrants the following, in relation to the Processing of Personal Data for its own Purposes in the context of the Services:

6.1. **EU/Swiss Data Transfers**

6.1.1. To the extent a Party receives Personal Data subject to the GDPR or FADP from the other Party and Processes (i) EU Personal Data in a country that is not subject to a European Commission adequacy decision or other adequacy finding or adequate safeguards referred to in Section 6.3 or (ii) Swiss Personal Data in a country that is not considered to provide for adequate data protection legislation by the Federal Council or subject to adequate safeguards referred to in Clause 6.3, the Parties agree that such transfers will be governed by the SCCs, which are hereby incorporated into this Addendum by reference, and completed as follows:

6.1.1.1. the signature to and dating of this Agreement shall constitute all required signatures and dates for the SCCs;

6.1.1.2. the text from module one of the SCCs shall apply and no other modules or any clauses marked as optional in the SCCs shall apply;

6.1.1.3. the information as required by Annex I of the SCCs is as set out in Annex 1 to Addendum A2 of the Agreement and the signatures for the purpose of Annex I of the SCCs are the signatures to this Agreement and the date is the date of this Agreement;

6.1.1.4. the technical and organisational measures required by Annex II of the SCCs are as set out in Appendix 1 of Controller to Controller terms of this Data Processing Agreement;

6.1.1.5. any notice provided under clause 14(e) or clause 16 of the SCCs shall be provided according to the timing and to the email address as set out in Clause 4.6 of this Data Processing Agreement;

6.1.1.6. for the purposes of clause 17 of the SCCs, option 1 applies and the SCCs shall be governed by the Laws of Belgium and for the purposes of clause 18 of the SCCs, the courts of Belgium shall have jurisdiction in relation to the SCCs; and

6.1.1.7. notwithstanding anything contrary in this Agreement or the Existing Agreement, clause 5 of the SCCs shall apply and, as such, in the event of a contradiction between the SCCs and the provisions of this Agreement or the Existing Agreement, the SCCs shall prevail.

6.1.1.8. In respect of Swiss Personal Data, (i) in deviation of clause 13 (a) of the SCCs in connection with its Annex I.C., the competent supervisory authority in Annex I.C. shall be the Swiss Federal Data Protection and Information Commissioner and all references to the "competent supervisory authority" shall be interpreted accordingly; (ii) in deviation of clause 17 of the SCCs, the SCCs, shall be governed by and construed in accordance with the substantive laws of Switzerland; (iii) in deviation of clause 18 (a) and (b) of the SCCs, any disputes arising from the SCCs shall be subject to the exclusive jurisdiction of the ordinary courts of Zurich, canton of Zurich, Switzerland; (iv) any references to "Regulation (EU) 2016/679"" and specific articles thereof in the SCCs should be interpreted to refer to the FADP and its corresponding provisions, as applicable; (v) in supplementation of clause 8.7 of the SCCs, 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 (vi) the term "member state" shall 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) and clause 18(c) of the SCCs shall be interpreted accordingly.

6.2. **UK Data Transfers**

6.2.1. To the extent a Party receives any Personal Data subject to the UK GDPR from the other Party and Processes such Personal Data in a country that is not subject to a UK government adequacy decision ("**UK Transfers**"), the Parties agree that such UK Transfers shall be governed by the UK Addendum, which is hereby incorporated into this Addendum by reference, but 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: (i) the details of the parties as set out in Table 1, and their signatures are included in the Annex 2 of Addendum A2 of the Agreement ; (ii) in Table 2, the first option is selected and the "Approved EU SCCs" are those incorporated into this DPA as per Section 6.1; (iii) in Table 3, "Annex 1A, 1B and 2 to the Approved EU SCCs" are Annex 2 to Addendum A2 of the Agreement and Appendix 1 of Controller to Controller terms of this Data Processing Addendum, respectively; and (iv) in Table 4, (iv) The UK Transfers shall be governed by the laws of England and Wales and any dispute arising from it shall be resolved by the courts of England and Wales. The Parties agree, notwithstanding anything to the contrary in the Existing Agreement, that Mastercard may make any amendments to the application of the EU Standard Contractual Clauses, the application of the UK Addendum and/or any other amendments to this Clause 6.2 of this Data Processing Agreement in respect of UK Transfers as it deems necessary to implement any replacement standard contractual clauses approved for use under Article 46 of the UK GDPR by notifying the Supplier of any such amendments to this Agreement in writing and such amendments shall be effective upon such notice.

6.3. Both Parties may transfer the Personal Data Processed in connection with the Services outside of Europe in accordance with European Data Protection Law, provided that the Personal Data are transferred to a country which provides an adequate level of protection under European Data Protection Law or to a data recipient which has implemented adequate safeguards under European Data Protection Law such as approved Binding Corporate Rules or SCCs. Mastercard will abide by the Mastercard BCRs when Processing Personal Data for its own Purposes in the context of the Services. Supplier acknowledges that Mastercard may transfer Swiss Personal Data globally.

6.4. **Data Disclosures.**

The Parties will only disclose Personal Data Processed to a third party in the context of the Services in accordance with European Data Protection Law and will require such third party in writing to comply with European Data Protection Law as well as the same obligations as are imposed on by this Addendum, as appropriate and relevant, unless it is not possible to do so, such as where the data recipient is a governmental authority.

7. Security of the Processing, Confidentiality, and Personal Data Breach Notification. Supplier agrees and warrants that:

7.1. it has implemented and maintains a comprehensive written information security program that complies with Privacy and Data Protection Law and Appendix 1 of Controller to Controller terms of this Data Processing Agreement and, to the extent Supplier Processes payment card information, the applicable Payment Card Industry Data Security Standards. Supplier's written information security program must include appropriate technical, operational and organizational measures to to ensure a level of security appropriate to the risk, which includes at the minimum the security measures listed in Appendix 1 of Controller to Controller terms of this Data Processing Agreement and as appropriate: (a) the pseudonymization and encryption of Personal Data (including the encryption of Primary Account Number (PAN) in transit and in rest); (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services (including by appropriately maintaining and reviewing logs, performing periodic password renewal and applying multi-factor authentication, in accordance with the controls referenced in Appendix 1 of Controller to Controller terms of this Data Processing Agreement; (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 of Personal Data. In assessing the appropriate level of security, Supplier 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, deletion, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise Processed ("**Information Security Program")**.

7.2. Supplier's Information Security Program must, among other things, include regular testing or otherwise monitoring of the effectiveness of Supplier's information safeguards. Supplier undertakes to notify Mastercard of any technical, operational, organizational or other change having a material impact on the security, confidentiality or protection of Personal Data Processed in the context of the Services, no less than 15 (fifteen) working days prior to implementing any such change. Supplier agrees to submit its Information Security Program to an audit in accordance with the Data Protection and Security Audit as provided under Section 8 of this Data Processing Agreement.

7.3. Supplier must take steps to ensure that any person (whether an individual, a legal entity or any other organization) acting under its authority who Processes or in any way has access to Personal Data in the context of the Services (including any person engaged by Supplier or any further Sub-Processor) is only granted access to Personal Data on a need-to-know basis and is subject to a duly enforceable contractual or statutory confidentiality obligation ("**confidentiality**").

7.4. Supplier must notify Mastercard of any Personal Data Breach or where there is a reasonable suspicion that such a Personal Data Breach has occurred i) by contacting the Mastercard Security Operations Center at +1-636-722-3600 or 1-800-358-3060 (US toll-free number) and/or; ii) in writing to SOC@mastercard.com, TPRM@mastercard.com and the account manager or main contact person of Mastercard specified under this Agreement, without undue delay, and no later than 24 (twenty-four) hours (or a shorter period of time if required by Privacy and Data Protection Law) after having become first aware of a Personal Data Breach or the reasonable suspicion of a Personal Data Breach, whichever is the earlier. Such notice will summarize in reasonable detail the effect on Mastercard, if known, of the Personal Data Breach, the corrective actions taken, and other information as required by Privacy and Data Protection Law. Supplier agrees to cooperate with Mastercard in all reasonable and lawful efforts to prevent, mitigate, investigate or rectify such Personal Data Breach including in relation to any forensic investigation or related audit

requested by Mastercard. Supplier will assist Mastercard in complying with its own obligations under Privacy and Data Protection Law to notify a Personal Data Breach. In case of conflict between this Section 7.4 and Section 8, this Section 7.4 will prevail.

7.5. Except to the extent prohibited by applicable legal, regulatory or law enforcement requirements, Supplier must obtain the written approval of Mastercard prior to the publication or communication of any filings, communications, notices, press releases or reports related to any Personal Data Breach that expressly mention Mastercard or its Affiliates. Supplier acknowledges and agrees that a violation of this section, or the occurrence of any Personal Data Breach, may cause immediate and irreparable harm to Mastercard for which damages may not constitute an adequate remedy. Therefore, Supplier agrees that Mastercard may seek injunctive or other equitable relief for any such violation or incident, in addition to its remedies at law, without proof of actual damages ("**personal data breaches**").

8. Data Protection and Data Security Audit

8.1. Upon request by Mastercard and subject to Mastercard's reasonable discretion, Supplier allows Mastercard or an inspection body composed of independent members to audit and review Supplier's Information Security Program, data processing facilities, and data protection compliance program to verify compliance with this Agreement (including with the security measures referenced in Appendix 1 of Controller to Controller terms of this Data Processing Agreement) and Privacy and Data Protection Law ("**Data Protection and Security Audit**").

8.2. The Parties will mutually agree upon the scope, timing, and duration of the Data Protection and Security Audit. Such Data Protection and Security Audit may be conducted by an independent third party auditor designated by Mastercard, in which case Supplier will within a reasonable time make available to Mastercard (a) the result of the Data Protection and Security Audit and (b) written confirmation that the Data Protection and Security Audit has not revealed any vulnerability or non-compliance, or, to the extent that any such vulnerability or non-compliance was revealed, written proof that it has been fully remedied.

8.3. Supplier agrees to fully cooperate with such Data Protection and Security Audit and implement all state of art industry standards to its Information Security Program, data processing facilities and data protection compliance program that, as a result of the Data Protection and Security Audit, are required to ensure Supplier's compliance with this Agreement and Privacy and Data Protection Law. Supplier's failure to allow or cooperate to any Data Protection and Security Audit, implement any required changes to its Information Security Program, data Processing facilities and other data protection compliance program and to provide the documentation as required in section 8.2, shall entitle Mastercard to suspend and terminate any further Personal Data Processing and terminate the Agreement, if doing so is required to or would be reasonably expected by Mastercard to be required to comply with the Agreement, Privacy and Data Protection Law, and as applicable with Mastercard's own obligations.

8.4. Upon request by Mastercard, Supplier must provide a certification of compliance with applicable Privacy and Data Protection Law and information security standards, such as the Payment Card Industry Data Security Standards (PCI-DSS) and SOC2 and ISO certifications, as applicable ("**Certification of Compliance**").

8.5. **Liability**

8.5.1. Each Party agrees that, in relation to the Processing of Personal Data for its own Purposes, it is fully liable towards Data Subjects, competent Government Bodies or other third parties for the entire compensation, damages or fines resulting from its own violation of Privacy and Data Protection Law or of this Agreement.

8.5.2. The Parties agree that if Mastercard has paid compensation, damages or fines, has been imposed an obligation to pay, or has otherwise been held liable for payment of any compensation, damages or fines to any Data Subject, competent Government Body or other third party due to any violations or breaches by Supplier of Privacy and Data Protection Law or of this Agreement (including but not limited to failure to provide the required cooperation and assistance), Mastercard is entitled to claim back from Supplier that part of the compensation, damages or fines, corresponding to Supplier's part of responsibility for the compensation, damages or fines.

9. Applicable law and jurisdiction. Subject to clauses 6.1.1.8 and 6.2.1, The Parties agree that the Processing will be governed by the Law of Belgium and that any dispute will be submitted to the Courts of Brussels.

10. Parties to Data Processing Agreement. Where the Processing of Personal Data is subject to EU Data Protection Laws or where EU SCCs apply, Mastercard Europe S.A. is the signatory to this Exhibit and the EU SCCs.

11. **Change in Law.** Mastercard will amend this Data Processing Agreement as reasonably necessary from time to time to update and address the requirements of Privacy and Data Protection Law.

APPENDIX 1: SECURITY MEASURES

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

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Supplier will, as a minimum, implement the security measures listed in "Security Requirements for Suppliers and Business Partners" at https://procurement.mastercard.com/information_suppliers.html, as may be updated from time to time. These security measures must be implemented in addition to any standards, certifications or audit requirements that Supplier adheres to (or has been certified to) with regard to the Services or Deliverables, including but not limited to the Payment Card Industry Data Security Standards (PCI-DSS) and ISO certifications, as applicable.

APPENDIX 2: REGION SPECIFIC PRIVACY TERMS

1. **China Data Processing Addendum**. The Parties agree that they will amend and supplement the terms as provided by Mastercard for the purposes of compliance with Privacy and Data Protection Law of the PRC if there is cross border transfer of Personal Data subject to the Privacy and Data Protection Law of the People's Republic of China ("China" or the "PRC", for the purposes of this Agreement, exclusive of Hong Kong Special Administrative Region, Macau Special Administrative Region and Taiwan).

2. **Japan Data Processing Addendum.** The Parties agree that they will amend and supplement the terms as provided by Mastercard for the purposes of compliance with Privacy and Data Protection Law of Japan in the event where (i) Mastercard conducts, in Japan, Processing of Personal Data of data subjects located in or out of Japan, and Supplier conducts in or out of Japan Processing of the said Personal Data pursuant to this Agreement, or (ii) Supplier Processes, in or out of Japan, Personal Data of data subjects located in Japan pursuant to this Agreement.

3. **CCPA.**

Additional Definitions.

- "CCPA" means the California Consumer Privacy Act of 2018, as amended, including as amended by the California Privacy Rights Act of 2020, together with all implementing regulations.

- The terms "business", "business purpose", "consumer", "personal information", "processing", "sale", "sell", "service provider", and "share" have the meanings given in the CCPA, where CCPA is applicable.

4. **Compliance**. (i) Supplier will provide the level of privacy protection required by CCPA, and (ii) where applicable, further represents and warrants that it understands and will comply with this Agreement. Supplier will Process Personal Data in compliance with this Agreement and CCPA. Supplier will notify Mastercard if, Supplier is unable to meet its obligations under the CCPA and this Agreement.

5. **Argentine Data.** In the event Personal Data subject to the Argentina Personal Data Protection Act 25.326 (PDPA) (Ley de Protección de los Datos Personales) is processed, the parties undertake to comply with the obligations applicable to a data controller set forth in the model contract titled Contrato Modelo de Transferencia Internacional de Datos Personales con Motivo de Cesión de Datos Personales adopted by the Data Protection Agency of the Republic of Argentina under Disposition 60 — E/2016 (the 'Argentinian SCCs') for the transfer of personal data to third countries.