DATA PROCESSING AGREEMENT

This Data Processing Agreement ("**DPA**") is entered into by and between Visa and its Affiliates ("Visa") and the Supplier and its Affiliates identified in the Agreement and/or on the face of the purchase order. This DPA is effective as of the date of the Agreement. This DPA applies to all Processing of Personal Information under the Agreement and is intended to demonstrate compliance with applicable privacy, security, and data protection laws. For the avoidance of doubt, Supplier agrees that it will ensure its Sub-processors comply with the requirements of this DPA as if they were Supplier.

1. **Definitions**. The following capitalized terms have the meanings provided below and, where applicable, will be interpreted based on the definitions given to them in the Privacy Laws. Capitalized terms not defined below shall have the meaning set forth in Definitions Exhibit to the Agreement. Regardless of any conflict between a definition in this DPA and a definition elsewhere in this Agreement, the definition in this DPA will apply to the term as used in this DPA. For the avoidance of doubt, the terms "Controller", "Personal Information", "Processing", "Processor", etc. below may be given different names and definitions in applicable Privacy Laws and should be interpreted and applied in accordance with such applicable Privacy Laws.

   1.1 "**Cardholder Information**" or "**Cardholder Data**" means, with respect to a payment card or other payment technology: (i) the account holder's name, PAN or account number, service code, card validation code/value, PIN or PIN block, valid to/from dates and/or magnetic stripe data and (ii) information relating to a payment transaction that can be associated with a specific account.

   1.2 "**Controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Information.

   1.3 "**Data Breach**" means a "personal data breach" (as defined in the GDPR or any other applicable Privacy Law), a "breach of the security of a system" or similar term (as defined in any other applicable Privacy Law) or any other event that compromises the security, confidentiality or integrity of any Personal Information. Data Breach includes, for example, incidents that involve unauthorized, unlawful, or accidental use, disclosure, loss, alteration, destruction of, or access to any Personal Information.

   1.4 "**Data Subject Request**" means any request by an individual (or by another person acting on behalf of an individual) to exercise a right under any Privacy Law, or any other complaint or inquiry or similar communication about the Processing of the individual's Personal Information.

   1.5 "**EEA Standard Contractual Clauses**" means the Standard Contractual Clauses set out in the European Implementing Decision (EU) 2021/914 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679, as amended or replaced from time to time by a competent authority under the relevant Privacy Laws, including the Swiss amendments to the EU Standard Contractual Clauses required by the Swiss Federal Data Protection Information Commissioner (the "**Swiss Addendum**") to the extent applicable.

   1.6 **"European Personal Data"** means personal data (as defined in GDPR) subject to the laws of the European Economic Area (EEA), Switzerland and the United Kingdom.

   1.7 "**GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 and any national data protection laws implementing that Regulation.

   1.8 "**Personal Information**" or "**PI**" means any data Processed in connection with the performance of the Services that is protected as "personal data", "personally identifiable information" or "personal information" under Privacy Laws, including any and all information that (alone or when used in combination with other information) is capable of being associated with, or could reasonably be associated with, an individual. Personal Information includes obvious identifiers (such as names, addresses, email addresses, phone numbers and identification numbers) as well as Cardholder Data, biometric data, and any and all information about an individual's computer or mobile device or technology usage, including (for example) IP address, MAC address, unique device identifiers, unique identifiers set in cookies, and any information passively captured about a person's online activities, browsing, application or hotspot usage or device location. For the avoidance of doubt, this

includes data relating to legal entities, if and as long as they are protected under the Swiss DP Laws.

1.9 "**Personnel**" means a Party's employees, agents, consultants, contractors, and Subcontractors, together with the personnel of any of the foregoing.

1.10 "**Privacy Law(s)"** means any applicable law, regulation, rule or other mandatory legal obligation which regulates the Processing of Personal Information or that otherwise relates to data protection, data security or Data Breach notification obligations for Personal Information, including (without limitation and only as applicable between the Parties) the U.S. Gramm-Leach-Bliley Act ("**GLBA**"); the GDPR; the UK GDPR; Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; the Canadian Personal Information Protection and Electronic Documents Act ("**PIPEDA**"); the Australian Privacy Act 1988 (including the Australian Privacy Principles); the California Consumer Privacy Act ("**CCPA**") as amended, superseded or updated from time to time; the Brazilian General Data Protection Law (Law 13.709/2018) ("**LGPD**"); the Personal Information Protection Law of the People's Republic of China ("**PIPL**") and similar laws.

1.11 "**Processing**" means any operation or set of operations that is performed upon Personal Information or on sets of Personal Information, whether or not by automated means, such as collection, recording, structuring, storage, alteration, accessing, consultation, use, copying, disclosure, combination, de-identification, redaction, erasure or destruction. ("**Process**", "**Processes**" and "**Processed**" are construed accordingly.)

1.12 "**Processor**" means a natural or legal person, public authority, agency or other body which Processes Personal Information on behalf of the Controller.

1.13 **"Relevant Services"** means any and all products or services provided by Supplier under the Agreement which involve the Processing of Personal Information.

1.14 "**Security Event"** means any actual or reasonably suspected unauthorized access, use, destruction, alteration, or disclosure of Visa Data, including any Personal Information provided by Visa, in the possession of Supplier or its third party service providers, or any such event alleged by a third party, whether an external actor or potential insider threat. For avoidance of doubt, the term "Security Event" includes any actual or reasonably suspected "Data Breach" or equivalent as defined in applicable Privacy Law.

1.15 "**Sub-processor**" or "**Subprocessor**" means a third party, including an affiliate of Supplier, that Processes Personal Information in the course of providing services to Supplier or that has access (even inadvertent access) to any Personal Information. For the avoidance of doubt, Sub-processors are considered Subcontractors.

1.16 **"Swiss DP Laws**" means the Federal Act on Data Protection of June 19, 1992 (as updated, amended and replaced from time to time), including all implementing ordinances.

1.17 "**Transfer**" means to transmit or otherwise make any Personal Information available across national borders in circumstances which are restricted by Privacy Laws, whether to Supplier, or to a third party (including to any Affiliate or Sub-processor), either by physical movement of the Personal Information to such third party or by enabling remote access to the Personal Information by other means.

1.18 "**UK GDPR**" means the GDPR as transposed into United Kingdom national law by operation of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019.

1.19 **"UK IDTA"** means the International Data Transfer Addendum to the EEA Standard Contractual Clauses issued by the UK Information Commissioner under section 119A(1) Data Protection Act 2018.

1.20 "**Visa Systems**" means all technology solutions and equipment, all associated or interconnected network equipment, routers, embedded software, and communication lines, and all components of any information system or equipment owned or operated by, or operated on behalf of, Visa, its Affiliates, or any Visa Client.

2. **Processing of Personal Information**. Supplier will Process Personal Information only as necessary to perform under the Agreement, in accordance with Visa's or Visa's Affiliates' written instructions or as needed to comply with law. Annex 1 contains the subject matter and a general description of the Processing activities to take place under the Agreement, including contact information for those Supplier Personnel who have primary responsibility for privacy and data security. Supplier will update Annex 1 and provide the updated version to Visa as needed to inform Visa of any changes, including any changes to the privacy and security contacts, Sub-processors, and Transfers. The Parties agree that the Agreement and this DPA set out Visa's complete and final instructions to Supplier in relation to the processing of Personal Information.

3. **Scope and Roles of the Parties**. The Parties hereby acknowledge and agree that depending on applicable Privacy Law, Visa is the Controller or Business, and Supplier is acting on behalf of Visa as the Processor or Service Provider with respect to the Personal Information, except where Visa acts as a Processor of Personal Information, in which case Supplier is a Sub-processor.

4. **Compliance**. Each Party must use reasonable efforts to stay informed of the legal and regulatory requirements for its Processing of Personal Information. Visa will comply with those obligations under Privacy Laws applicable to it as a Controller and Supplier will comply with those obligations under Privacy Laws applicable to it as a Processor. Supplier will promptly notify Visa if, in its opinion, the instructions given by Visa or its Affiliates for Processing violate any law. Supplier will also promptly notify Visa of any circumstances that may prevent it or any Sub-processor from complying with its obligations under any applicable Privacy Law or this DPA.

5. ***Specific Compliance Requirements.*** To the extent applicable:

   5.1 **CCPA**: In the event that Supplier processes Personal Information subject to the CCPA or any similar applicable U.S. State consumer privacy act, Supplier agrees to the terms set forth in Annex 3.

   5.2 **HIPAA:** If the Personal Information includes "protected health information" as defined in the U.S. Heath Information Portability and Accountability Act ("**HIPAA**"), Supplier and Visa agree that the Visa Business Associate Agreement Terms are incorporated herein as required by HIPAA.

   5.3 **European Personal Data:** If the Personal Information includes European Personal Data, Supplier and Visa will ensure adequate protection for the European Personal Data. The Parties will ensure adequate protection for any Transfers of European Personal Data using the mechanism(s) indicated in Annex 2 and (as applicable) **Additional Protections for European Personal Data Addendum** located at https://usa.visa.com/partner-with-us/info-for-partners/info-for-suppliers.html. In the event that relevant authorities or courts determine that the Transfer mechanism selected is no longer an appropriate basis for Transfers, Supplier and Visa will promptly take all steps reasonably necessary to demonstrate adequate protection for the European Personal Data using another approved mechanism.

   5.4 **Brazil PI:** If the Personal Information includes any Personal Information subject to the laws of Brazil, Supplier acknowledges that such Personal Information is subject to the LGPD. The Parties will ensure adequate protection for any Transfers of Personal Information subject to the LGPD using the mechanism indicated in Annex 2.

   5.5 **China PI:** If the Visa Data includes any Personal Information subject to the laws of China, Supplier acknowledges and confirms that its Processing of such Personal Information shall be in compliance with the relevant provisions under the PIPL, including, without limitation, provisions related to jointly processing, entrusting others to process, providing Personal Information to other Processors, and localizing and cross-border transferring of the Personal information.

   5.6 If performance under the Agreement involves Supplier's collection of Personal Information on behalf of Visa directly from individuals, Supplier will provide the individuals with a clear and conspicuous privacy notice, which notice will either be (i) Visa's or its Affiliate's privacy notice, or (ii) Supplier's privacy notice, provided that such notice must address any legal requirements for such notices in the jurisdictions where it is given, be translated into the languages regularly used in connection with Supplier's interaction with the individuals, and indicate that Supplier is Processing the data as a Processor on behalf of its customers. All such notices must be approved by Visa.

   5.7 Supplier represents and warrants that neither it nor any employee, agent, or subcontractor that will

access, Process, or store "bulk U.S. sensitive data" or U.S. "government-related data" under this Agreement is a "Covered Person" as those terms are defined in 28 Code of Federal Regulations (CFR) 202.211 and any U.S. Department of Justice guidance or interpretation relating to that regulation. Supplier shall notify Visa in writing of any change to the foregoing representation within 48 hours of such change. In such event, Visa shall have the right to immediately terminate the Agreement. In addition to Supplier's obligations under the Agreement, Supplier shall not transfer, sell, or license access to, or engage in any similar commercial transaction involving the transfer of Personal Information to any Covered Person. Supplier will, upon request, provide any information reasonably necessary for Visa to comply with the requirements of 28 CFR Part 202. Such information includes but is not limited to: (i) documentation, information, and materials; (ii) representations related to the Covered Data, and (iii) records related to activities involving Covered Data, including its transfer, access, and processing.

6. **Supplier Personnel**. Supplier will limit access to the Personal Information to its Personnel that need to access Personal Information to perform under the Agreement. Prior to allowing Personnel to Process Personal Information, Supplier will (i) conduct an appropriate background investigation of the individual as permitted by law (and receive an acceptable response), (ii) require the individual to execute an enforceable confidentiality agreement, and (iii) provide the individual with appropriate privacy and security training. Supplier will also monitor its Personnel for compliance with this DPA and apply appropriate disciplinary measures for individuals that fail to comply.

7. **Additional Requirements for Supplier Personnel with Access to Visa Facilities or Systems**. For all Supplier Personnel who perform unescorted services onsite at a Visa or Visa Affiliate facility or who have access to Visa Systems:

   7.1 As permitted by applicable law, Supplier will cause such Personnel to submit to background investigations by Visa or its designee, including criminal history and providing evidence of the person's right to work in the particular location where the Relevant Services are being performed. Supplier will obtain written consents from such Personnel as may be necessary to conduct such investigations and provide these to Visa upon request.

   7.2 Supplier will ensure that such Personnel complete training on Visa's or its Affiliates' "key controls" and operational and security standards, as may be provided by Visa or its Affiliates, within thirty (30) days of being granted access to such systems and annually thereafter. Supplier will keep an updated list of those Personnel who have completed the training and provide Visa with this list upon request.

8. **Data Security**. Supplier will implement and maintain a comprehensive, written information security program that includes appropriate administrative, technical, physical, and organizational safeguards designed to (i) ensure the privacy, confidentiality and security of Personal Information, (ii) protect against any anticipated threats or hazards to the security and integrity of Personal Information and Visa Systems, and (iii) protect against unauthorized access to, or acquisition or use of, Personal Information and Visa Systems. Supplier's security program will include, and comply with, all measures identified in the **Visa Supplier Security Standards** located at https://usa.visa.com/partner-with-us/info-for-partners/info-for-suppliers.html, comply with applicable Privacy Laws, reflect industry best practices, and include any additional measures that are specified in the Agreement.

9. **Transfers of Personal Information**. Visa approves the Transfers described in the Agreement and/or in Annex 1and 2. Any Transfers made shall be carried out in accordance with the requirements of the relevant Privacy Laws. Supplier will not make other Transfers nor permit the Transfer of any Personal Information without the prior written consent of Visa ("**Approved Transfer**") or deemed consent as described in Section 10 (Sub-processors). Supplier will notify Visa thirty (30) days prior to any proposed Transfer in addition to those described in Annex1 and 2, providing Visa with all information required to complete an assessment of the proposed Transfer under Privacy Laws. Visa will evaluate the proposed new Transfer and notify Supplier of any objections or additional legal requirements. Supplier will not undertake such Transfers until such objections or requirements have been addressed to Visa's reasonable satisfaction.

10. **Sub-processors**.

    10.1 Supplier will provide Visa with a list of all Sub-processors (the "**Sub-processor List**") as at the date of the Agreement in the form set out in Annex 1, or on the website referenced in Annex 1. Visa

authorizes Supplier to engage the Sub-Processors listed in Annex 1. Supplier will not authorize any additional Sub-processors to Process the Personal Information without Visa's prior consent as described in this Section. For each of its Sub-processors, Supplier will:

(A) Conduct adequate due diligence on the Sub-processor to ensure that it is capable of providing the level of protection for Personal Information as is required by this Agreement;

(B) Enter into a written contract with the Sub-processor that includes terms equivalent to those contained in this Agreement (offering the same level of protection for Personal Information) and provides that the Sub-processor's right to Process Personal Information can be terminated by Supplier immediately on expiry or termination of the Agreement for whatever reason; and

(C) Remain primarily liable to Visa and Visa's Affiliates for the acts, errors and omissions of the Sub-processor, as if they were Supplier's own acts, errors, and omissions.

10.2 Supplier will notify Visa thirty (30) days prior to any proposed addition of a new Sub-processor. Visa will evaluate proposed new Sub-processors and notify Supplier within thirty (30) days (i) if the addition is approved or (ii) of any objection. If Visa fails to respond within 30 days, the new Sub-processor will be deemed approved by Visa. Supplier will not allow such Sub-processor to access any Personal Information until the objection is addressed to Visa's reasonable satisfaction.

10.3 Upon request, Supplier will provide Visa with a then-current copy of the Sub-processor List along with copies of the due diligence it conducted and its agreements with its Sub-processors (which may be redacted to remove confidential commercial information not relevant to compliance with these Terms).

11. **Third-Party Requests for Personal Information**. If Supplier receives any subpoena, order, demand, warrant, or any other document requesting or purporting to compel the production of Personal Information (a "**Third-Party Request**"), Supplier will (unless prohibited by law) promptly notify Visa. If the Third-Party Request is not legally valid and binding, Supplier will not respond to it. If a Third-Party Request is legally valid and binding, Supplier will use good faith efforts to provide Visa at least forty-eight (48) hours' notice prior to the required disclosure, so that Visa or its Affiliates may exercise any rights as it may have under applicable law to prevent or limit such disclosure. Notwithstanding the foregoing, Supplier will exercise commercially reasonable efforts to prevent and limit any such disclosure and to otherwise preserve the confidentiality of Personal Information. Supplier will also cooperate with Visa and Visa's Affiliates with respect to any action taken with respect to such Third-Party Request, including to obtain an appropriate protective order or other reliable assurance that confidential treatment will be accorded to Personal Information. In all cases, Supplier will provide a copy to Visa of all Personal Information and any relevant information that it does so disclose unless prohibited by applicable law.

12. **Data Subject Requests**. Supplier will promptly notify Visa of any Data Subject Requests by sending an email to privacy@visa.com. Unless otherwise agreed (such as for handling of requests contemplated by the Agreement), Visa or its Affiliates will handle Data Subject Requests, and Supplier will not disclose any Personal Information in response to any such requests, except to the extent Supplier is required to do so under applicable law. Supplier will reasonably assist Visa with Data Subject Requests as may be required to comply with applicable Privacy Laws. Should Supplier be legally obligated to respond to a Data Subject Request, it will also provide a copy to Visa of all Personal Information and any relevant information that it discloses.

13. **Data Protection Impact Assessments and Prior Consultation with Regulator**. As may be required by Privacy Laws, Supplier will reasonably assist Visa and Visa's Affiliates with any data protection impact assessments and prior consultations with regulators, in each case solely in relation to Processing of Personal Information by Supplier.

14. **Return, Deletion and Retention**. When Supplier ceases to perform under the Agreement (and at any other time, upon request), Supplier will either (i) purge, delete and destroy the Personal Information and/or (ii) at Visa's request, return the Personal Information (and all media containing copies of the Personal Information). Electronic media containing Personal Information will be disposed of in a manner that renders the Personal Information unrecoverable. Upon request, Supplier will provide Visa with an officer's certificate to certify compliance with this provision. If Supplier is required by applicable law to retain any Personal

Information, Supplier warrants that it will (i) ensure the continued confidentiality and security of the Personal Information, (ii) securely delete or destroy the Personal Information when the legal retention period has expired, and (iii) not actively Process the Personal Information other than as needed to comply with law.

15. **Accountability and Audits**. Upon request, Supplier will provide Visa with information reasonably needed to demonstrate compliance with the obligations in this DPA and allow for (and contribute to) audits, including inspections conducted by Visa or another auditor under the instruction of Visa as may be required by the Privacy Laws. Supplier will also cooperate with any supervisory authority audit or investigation regarding its (or its Sub-processors) Processing of Personal Information.

    Visa and its Affiliates reserve the right from time to time to conduct detailed security and risk assessments ("**Assessments**") of Supplier which may include an onsite assessment by Visa (or its designated agent) to verify Supplier's compliance with this DPA. Assessments will be conducted during normal business hours. Supplier agrees to reasonably cooperate with Visa or its Affiliate during any such Assessment. In the event that an Assessment reveals material gaps or weaknesses in Supplier's security program, Supplier agrees to work with Visa, in good faith and at Supplier's expense, to resolve the issues. Visa and its Affiliates will be entitled to suspend Supplier's Processing of Personal Information until such issues are resolved.

16. **Data Breaches**. In accordance with the Security Event provision of the **Visa Supplier Security Standards,** Supplier will promptly and thoroughly investigate all alleged or suspected instances of unauthorized access to, use or disclosure of or alteration or destruction of the Personal Information ("**Data Breach**") and will report any event reasonably believed to constitute a Data Breach to Visa. Supplier will notify Visa of any Data Breach in writing without undue delay, no later than twenty-four (24) hours after discovery of the Data Breach. This notification must be made via email to vsirt@visa.com.

17. **Third-Party Beneficiaries**. Supplier agrees that Visa's Affiliates and, where applicable, corporate customers, are intended third-party beneficiaries of this DPA. Without limiting the foregoing, the intended third-party beneficiaries will be entitled to enforce this DPA directly, or Visa or its Affiliates may enforce it on behalf of the intended third-party beneficiaries. Notwithstanding the rights of these third-party beneficiaries, Supplier will be entitled to rely solely on Visa's instructions regarding the Processing of the Personal Information.

18. **Conflicts and Consideration**. This DPA supersedes any conflicting provision of the Agreement related to the Processing of Personal Information. A violation of this DPA will constitute a material breach of the Agreement.

19. **Term and Survival**. The obligations of Supplier under this DPA will continue for so long as Supplier Processes Personal Information, even if all other agreements between Supplier and Visa have expired or have been terminated.

ANNEX 1

[Note: Annex 1 is attached to the main body of the Agreement]

Annex 2
Transfers of Personal Information:

European Personal Data subject to the GDPR: For Transfers of European Personal Data to countries (or to territories or sectors within a country) or international organizations which do not benefit from an adequacy decision under the GDPR (including those whose adequacy decision is revoked by the European Commission):

A. *Binding Corporate Rules***.** If applicable, the Supplier will Transfer European Personal Data pursuant to its approved set of Binding Corporate Rules for Data Processors; OR

B. *Standard Contractual Clauses***.** Where the Supplier does not have an approved set of Binding Corporate Rules for Data Processors, the EEA Standard Contractual Clauses shall apply as follows:

   i. Where the Transfer is made between Visa and Supplier and Visa acts as Controller, Module 2 of the EEA Standard Contractual Clauses is hereby incorporated into this Agreement by reference and:

      a. Clause 7 – *Docking clause* shall apply;

      b. Clause 9 – *Use of sub-processors* Option 2 shall apply and the "time period" shall be 30 days;

      c. Clause 11(a) – *Redress* the optional language shall not apply;

      d. Clause 13(a) – *Supervision*

         Where Visa is established in an EU Member State, the following shall apply: "*The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority*".

      e. Clause 17 – *Governing law* Option 1 shall apply and the "Member State" shall be Ireland;

      f. Clause 18 – *Choice of forum and jurisdiction* the Member State shall be Ireland;

      g. Annex I – the data exporter is Visa and the data importer is Supplier (in each case as identified in this Agreement) and the processing operations are deemed to be those described above in this Annex 1 to this **Data Processing Agreement**.

      h. Annex I C. – Where Visa is established in an EU Member State, the competent supervisory authority is the Irish Data Protection Commission;

      i. Annex II – the technical and organizational security measures are those identified in the **Visa Supplier Security Standards**; and

      j. Annex III – Supplier's sub-processors are those identified in Annex 1 to this DPA (Sub-processor List).

   ii. Where the Transfer is made between Visa and Supplier and Visa acts as Processor, Module 3 of the EEA Standard Contractual Clauses is hereby incorporated into this Agreement by reference, and the options and Annex information described in (i)(a) to (i)(j) above shall apply *mutatis mutandis* to Module 3.

   iii. Where the Transfer is made between Supplier and a Sub-processor, Supplier shall enter into Module 3 of the EEA Standard Contractual Clauses directly with the Sub-processor.

C. *Additional Protections*. The additional contractual protections set out in **Additional Protections for European Personal Data Addendum** located at https://usa.visa.com/partner-with-us/info-for-partners/info-for-suppliers.html to this DPA shall apply to Transfers of European Personal Data subject to the GDPR.

European Personal Data subject to the UK GDPR: For Transfers of European Personal Data to countries (or to territories or sectors within a country) or international organizations which do not benefit from an adequacy decision under the UK GDPR:

A. *Binding Corporate Rules*. If applicable, Supplier will Transfer European Personal Data pursuant to its approved set of UK Binding Corporate Rules for Data Processors; OR

B. *Standard Contractual Clauses*. Where the Supplier does not have an approved set of UK Binding Corporate Rules for Data Processors, the EEA Standard Contractual Clauses, with the modules, clauses and optional provisions described in the section of this Annex titled "European Personal Data subject to the GDPR", shall apply and be read in accordance with, and deemed amended by, the provisions of Part 2 (Mandatory Clauses) of the UK IDTA (together, the "**UK SCCs**"). For the purposes of Table 4 in Part 1 (Tables) of the UK IDTA, the Parties select the "neither party" option. Otherwise, the Parties confirm that the information

required for the purposes of Part 1 (Tables) of the UK IDTA is set out in Annexes 1 and 2 to this DPA, and Exhibit F.

i. If there is any conflict or inconsistency between a term in the body of this DPA, the Agreement and a term in the UK SCCs incorporated into this Agreement, the term in the UK SCCs shall take precedence; and

ii. Where the Transfer is made between Supplier and a Sub-processor, Visa hereby authorizes Supplier to enter into the UK SCCs with any approved Sub-processor for and on its behalf (or, where applicable, on behalf of the relevant Visa corporate customer acting as Controller).

C. *Additional Protections*. The additional contractual protections set out in **Additional Protections for European Personal Data Addendum** to this DPA shall apply to Transfers of European Personal Data subject to the UK GDPR.

Personal Information Subject to Swiss DP Laws: Where the Transfer is subject to the Swiss DP Laws, the Section entitled "European Data Subject to the GDPR" shall apply except that the Parties agree on the following amendments to the EEA Standard Contractual Clauses:

A. The term "Member State" according to Clause 18 (c) of the EEA Standard Contractual Clauses shall not be interpreted in a such a way that data subjects in Switzerland are excluded from exercising their rights, if any, at their place of habitual residence;

B. The supervisory authority pursuant to Clause 13 of the EEA Standard Contractual Clauses is the Swiss Federal Data Protection and Information Commissioner;

C. The law applicable to the EEA Standard Contractual Clauses pursuant to Clause 17 of the EEA Standard Contractual Clauses shall be Swiss DP Laws;

D. The place of jurisdiction under Clause 18 (b) of the EEA Standard Contractual Clauses shall be the courts of the city of Zurich;

E. Where the EEA Standard Contractual Clauses include references to the GDPR, such references shall be understood as references to the Swiss DP Laws.

Personal Information Subject to the Laws of Argentina: For Transfers of Personal Information subject to the laws of Argentina ("**Argentine Personal Information**") to jurisdictions that are not considered by Argentina to provide adequate data protection, the Contrato modelo de transferencia internacional de datos personales con motivo de prestación de servicios published by the Argentine National Office for the Protection of Personal Data ("**Argentine Model Clauses**") shall apply as follows:

A. Where the Transfer is made between Visa and Supplier, the Argentine Model Clauses shall apply with respect to any transfer of Argentine Personal Information from Visa (or the applicable Visa affiliate, or a corporate customer) to Supplier. The Parties acknowledge and agree that:

i. The Argentine Model Clauses are hereby incorporated into the Agreement by reference;

ii. Visa (or the applicable Visa affiliate, or a corporate customer) will act as the "data exporter";

iii. Supplier will act as the "data importer"

iv. If there is any conflict or inconsistency between a term in the body of this DPA, the Agreement and a term in the Argentine Model Clauses incorporated into this Agreement, the term in the Argentine Model Clauses shall take precedence; and

v. The information in this Annex 1 is incorporated into Appendix 1 of the Argentine Model Clauses.

B. Where the Transfer is made between Supplier and a Sub-processor, Visa hereby authorizes Supplier to enter into the Argentine Model Clauses with any approved Sub-processor for and on its behalf (or, where applicable, on behalf of the relevant Visa corporate customer).

Personal Information Subject to the Laws of Brazil: For Transfers of Personal Information subject to the laws of Brazil ("**Brazilian Personal Information**") to jurisdictions which do not benefit from an adequacy decision under the LGPD, the standard contractual clauses published by the Brazilian Data Protection Authority ("**Brazilian Model Clauses**") shall, once made available, apply as follows:

A. Where the Transfer is made between Visa and Supplier, the Brazilian Model Clauses shall apply with respect to any transfer of Brazilian Personal Information from Visa (or the applicable Visa affiliate, or a corporate customer) to Supplier. The Parties acknowledge and agree that:
   i. The Brazilian Model Clauses are hereby incorporated into the Agreement by reference;
   ii. Visa (or the applicable Visa affiliate, or a corporate customer) will act as the "data exporter";
   iii. Supplier will act as the "data importer"
   iv. If there is any conflict or inconsistency between a term in the body of this DPA, the Agreement and a term in the Brazilian Model Clauses incorporated into this Agreement, the term in the Brazilian Model Clauses shall take precedence; and
   v. The information in Annex 1 is incorporated into Appendices of the Brazilian Model Clauses, as appropriate.

B. Where the Transfer is made between Supplier and a Sub-processor, Visa hereby authorizes Supplier to enter into the Brazilian Model Clauses with any approved Sub-processor for and on its behalf (or, where applicable, on behalf of the relevant Visa corporate customer).

Personal Information Subject to the Laws of China: For Transfers of Personal Information that are defined as cross-border activities subject to the laws of China ("**Chinese Personal Information Outbound Transfer**"), regardless of any such Transfer is between Visa (or the applicable Visa affiliate, or a corporate customer) and Supplier or between Supplier and a Sub-processor, the provisions of the relevant laws, regulations, and regulatory documents of China shall apply. In order to carry out the personal information protection impact assessment, self-assessment on the risks of the data cross-border transfer, any other work as required in accordance with the relevant laws, regulations, and regulatory documents of China, Supplier shall, in accordance with the instructions of Visa, provide relevant information, materials, and documents to Visa in a timely manner, sign relevant legal documents, cooperate with Visa to complete the relevant works, and ensure that all Sub-processors also, in accordance with the instructions of Visa, take the same actions. Depending on the Chinese Personal Information Outbound Transfer, the Parties agree to take the following actions:

A. Supplier shall provide such reasonable assistance to advise Visa whether there are any circumstances in which the Chinese Personal Information Outbound Transfer can be exempted from having to conclude a security assessment, a Standard Contract for Cross-border Transfer of Personal Information ("**China SCC**"), or a Personal Information protection certification (collectively, "**Exemption**"). If Visa agrees with the Supplier that an Exemption applies, the Supplier shall assist Visa to carry out any necessary work as may be required to assist Visa to secure a compliant Exemption. For the avoidance of doubt, Visa's decision as to whether an Exemption applies shall prevail.

B. Where Visa concludes that an Exemption does not apply, the Supplier shall, in accordance with Visa's direction, and at Supplier's own cost, undertake one of the following methods with respect to the Transfer of Personal Information:
   i. *Security Assessment:* cooperate with Visa to complete the security assessment at the cyberspace authority in China;
   ii. *Conducting the certification for personal information protection:* cooperate with Visa to apply for personal information protection certification to the certification body specified by the cyberspace authority in China; or
   iii. *China SCC:* cooperate with Visa or cause the relevant parties involved in the Chinese Personal Information Outbound Transfer to cooperate with Visa in concluding the China SCC.

ANNEX 3

U.S. STATE LAW COMPLIANCE REQUIREMENTS

As used in this Annex, the following terms have the meanings set forth in the California Consumer Privacy Act and its regulations ("CCPA") and similar applicable U.S. State consumer privacy acts along with their respective regulations (each a "CPA"): (1) Business Purpose; (2) Collect; (3) Commercial Purpose; (4) Sell and (5) Share.

1. When Supplier Collects or Processes Personal Information on behalf of Visa as a Processor, Service Provider or Contractor (or applicable term) that is subject to a CPA pursuant to this Agreement, Supplier:

   1.1 Agrees that Visa is disclosing, and Supplier will only process, the Personal Information for the following Business Purposes (*describe each purpose specifically; add as many as needed*):

   - As described in Annex 1, Description of Services;
   - _____

   1.2 Will not, except to the extent necessary to comply with Supplier's legal obligations: (1) Sell or Share Personal Information; (2) retain, use or disclose Personal Information for any purpose, including a Commercial Purpose, other than the Business Purposes specified in subsection 1.1 of this Annex; (3) retain, use, or disclose Personal Information outside the direct business relationship between the Parties hereunder; or (4) combine Personal Information processed under this Agreement with any other personal information, except as expressly allowed by the CPA.

   1.3 Certifies that it understands the restrictions contained in this Annex and will comply with them and agrees to notify Visa promptly and within any period required by law if it determines it can no longer meet its obligations under this paragraph or the CPA.

   1.4 Agrees that Visa (1) is neither Selling nor Sharing the Personal Information Supplier Collects pursuant to the Agreement and (2) has received nothing of value in return for such Personal Information.

   1.5 Will notify Visa if it engages any other person to assist it in processing Personal Information under this Agreement, or if any other person engaged by the Supplier engages another person to assist in processing Personal Information for that Business Purpose, and the engagement shall be pursuant to a written contract binding the other person to observe all the requirements set forth in this Annex.

   1.6 Will comply with all applicable sections of the CPA including, with respect to the Personal Information that it Collects pursuant to this Agreement, providing the same level of privacy protection as required of businesses by the CPA.

   1.7 Will promptly cooperate with Visa and provide the necessary assistance for Visa to respond to and comply with consumer or governmental requests made pursuant to the CPA. Notwithstanding the above, and as relevant under the circumstances, when Visa requests assistance in fulfilling a consumer request, Supplier will also notify and direct any third parties it utilizes for processing Visa's Personal Information under this Agreement to also action any such request on the relevant Personal Information.

   1.8 Will implement reasonable security procedures and practices appropriate to the nature of the Personal Information received from, or on behalf of, Visa to protect the Personal Information from unauthorized or illegal access, destruction, use, modification, or disclosure in accordance with California Civil Code section 1798.81.5, Virginia Code section 59.1-578 (3), or applicable CPA.

   1.9 Grants Visa the right to take reasonable and appropriate steps to ensure that Supplier uses the Personal Information that it Collected pursuant to this Agreement in a manner consistent with Visa's obligations under the CPA. Reasonable and appropriate steps may include ongoing manual reviews and automated scans of the service provider's system and regular internal or third-party assessments, audits, or other technical and operational testing at least once every 12 months.

   1.10 Agrees that Visa has the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized processing of Personal Information, without limitation or waiver to any rights

it has under this Agreement. For example, Visa may require Supplier to provide documentation that verifies that it no longer retains or uses the Personal Information of consumers that have made a valid request to delete.