

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.

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 Exhibit A 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 “**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.
 - 1.2 “**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, integrity, or availability of any Personal Information, including reidentification of any Deidentified data. Data Breach includes, for example, incidents that involve unauthorized, unlawful, or accidental use, collection, copying, modification, disposal, disclosure, loss, alteration, destruction of, or access to any Personal Information, including the loss of any storage medium or device on which Personal Information is stored. For purposes of this DPA, Data Breach is a subset of Security Event as defined in the Security Standards exhibit.
 - 1.3 “**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.
 - 1.4 “**Data Localization Requirement**” means any requirement under Applicable Law that mandates or restricts the storage, Processing, or Transfer of Personal Information to specified geographic locations or jurisdictions, including any data residency, data sovereignty, or data localization obligations.
 - 1.5 “**Deidentified**” means that (i) the Personal Information has all Direct Identifiers removed, (ii) the individuals cannot reasonably be identified using indirect identifiers or other information available to the Supplier, and (iii) the Supplier has a formal program containing administrative and technical controls that are reasonably designed to ensure that the resulting data are not re-identified or otherwise used in an identifiable manner by Supplier or any third party. For purposes of this definition, a “**Direct Identifier**” is any single data element that could reveal a person’s identity, such as a person’s name, username or online identifier, email address, physical address or geolocation, telephone number, device or vehicle identifier, birthdate, transaction date, identification number (such as a government-issued ID number or account number) payment card number, IP address, biometric identifier, photograph or other image that allows individual identification.
 - 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 “**High Risk Processing Activity**” means any processing activity that triggers the completion of a formal risk or impact assessment under any Privacy Law, including (without limitation), (i) processing in connection with or to train a high risk AI system (as defined in the Privacy Laws), (ii) the large-scale or systematic monitoring of individual or public spaces, (iii) biometric identification or biometric Profiling, (iv), the processing of sensitive or special categories of data, (v) Profiling to infer emotion or sensitive data, such as health conditions; (vi) Profiling based on person’s presence in a sensitive

location such as a healthcare facility, educational institution, legal service office or other place that indicates religion, political opinion or union membership, (vii) Profiling or other processing to support decision-making, when the decisions may have a legal or similarly significant effect on the individual, such as in education, employment, finance, healthcare, housing, insurance or legal services, (viii) processing that generates automated decisions that are significant or consequential, and (ix) any other processing that is otherwise regulated as a “high risk” by the Privacy Law.

- 1.9 **“Personal Information” or “PI”** means any data Processed 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 without limitation 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 Privacy Laws.
- 1.10 **“Privacy Law(s)”** means (to the extent applicable in respect of a Party’s obligations under the Agreement) 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; UK Data Protection Laws; Swiss DP Laws; 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**”); the Singapore Personal Data Protection Act 2012; the Japan Act on the Protection of Personal Information; the Korean Personal Information Protection Act; the Hong Kong Personal Data Privacy Ordinance; the New Zealand Privacy Act 2020; the Philippines Data Privacy Act, and similar laws and any associated regulations or any other legislation or regulations that transpose, supersede or are deemed substantially similar to the above. Privacy Laws also include (without limitation) any applicable laws or regulations that apply to any AI Systems developed or deployed by Supplier and used in connection with Supplier’s provision of Services under the Agreement, such as Regulation (EU) 2024/1689 (“**EU AI Act**”), the Vietnam Law on Artificial Intelligence (Law No. 134/2025/QH15) or the Korea AI Basic Act, similar laws and any associated regulations or any other legislation or regulations that transpose, supersede or are deemed substantially similar to the above.
- 1.11 **“Processing”** means Processing as defined in the Agreement, provided that for purposes of this DPA Processing is limited to Personal Information (“**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 **“Profiling”** means automated processing to evaluate, analyze or predict a natural person’s intelligence, ability, aptitude, performance at work or in school, economic situation, health, (including mental health), personal preferences, interests, reliability, predispositions, behavior, location, or movements, including by use of physical or biometric data, such as the analysis of facial expressions, voice recordings or similar characteristics.
- 1.14 **“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, Subprocessors are considered Subcontractors.

- 1.15 **“Transfer”** means a transfer of Personal Information (or an onward transfer) across national borders, regardless whether by physical movement of the Personal Information to the recipient or by enabling remote access to the Personal Information by other means, where such transfer would be prohibited by Privacy Laws in the absence of appropriate safeguard(s), valid adequacy decision or other lawful derogation, or otherwise subject to conditions, restrictions, or requirements under applicable Privacy Laws.
 - 1.16 **“UK Data Protection Laws”** 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 (**“UK GDPR”**), together with the Data Protection Act 2018, the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 and other data protection or privacy legislation in force from time to time in the United Kingdom. In this DPA, in circumstances where and solely to the extent that the UK GDPR applies, references to the GDPR and its provisions shall be construed as references to the UK GDPR and its corresponding provisions.
2. **Processing of Personal Information.** Supplier shall Process Personal Information only to the extent, and in such a manner, as is necessary to perform its obligations under the Agreement, in accordance with Visa’s or Visa’s Affiliates’ written instructions or as needed to comply with Supplier’s legal or regulatory obligations (provided that Supplier shall inform Visa of that legal requirement before undertaking such Processing of Personal Information unless such applicable laws prohibit such information on important grounds of public interest). Annex 1 contains the subject matter and general description of the Processing activities to take place under the Agreement, including contact information for Supplier’s Personnel who have primary responsibility for privacy and data security. Supplier shall have an ongoing obligation to update Annex 1 and provide the updated version to Visa as needed to inform Visa of any changes from time to time, including any changes to the privacy and security contacts, Subprocessors, and/or 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.**
 - 3.1 **General.** The Parties’ respective roles for Processing Personal Information under the Agreement are determined by applicable Privacy Laws and the specific Processing activities under this Agreement. References to Controller, Processor, and Subprocessor include, where applicable, analogous concepts under Privacy Laws, including Business, Service Provider, Third Party, or similar terms, in each case as applicable to the relevant Processing activity and Party role. For purposes of this Section 3 (Scope and Roles of the Parties), Personal Information may be provided by Visa, a Visa Client, an individual, Supplier, or a third party, and the applicable role configuration depends on the purposes and means of Processing, the applicable instructions, and the Processing activity documented in the Agreement, including this DPA. The source or method of collection of Personal Information, including direct collection by Supplier from individuals, does not by itself determine the Parties’ roles.
 - 3.2 **Supplier as Processor for Visa Internal Use (Visa as Controller).** Where Supplier Processes Personal Information for Visa’s internal purposes, or other purposes determined by Visa, Visa acts as Controller and Supplier acts as Processor. Supplier shall Process such Personal Information only in accordance with Visa’s documented instructions in the Agreement and this DPA.
 - 3.3 **Supplier as Processor for Visa External Use (Visa as Controller).** Where Supplier Processes Personal Information in connection with Visa products or services, or Supplier Services made available by or through Visa to Visa Clients or other external users, and Visa determines the purposes and means of such Processing, Visa acts as Controller and Supplier acts as Processor. Supplier shall Process such Personal Information only in accordance with Visa’s documented instructions in the Agreement and this DPA, regardless of whether such Personal Information is provided by Visa, a Visa Client, an individual, Supplier, or a third party.
 - 3.4 **Supplier as Subprocessor (Visa as Processor).** Where Visa Processes Personal Information as Processor on behalf of a Visa Client or other Controller, and Supplier Processes such Personal Information to support Visa’s Processing, Supplier acts as Subprocessor. Supplier shall Process

such Personal Information only in accordance with Visa's documented instructions in the Agreement and this DPA, including any applicable Controller instructions conveyed to Supplier through Visa.

- 3.5 **Direct Supplier–Visa Client Processing.** Where Supplier provides Services directly to a Visa Client under a separate written agreement between Supplier and that Visa Client, and the relevant Processing is outside Visa's role under the Agreement, the Visa Client and Supplier are responsible for determining and documenting their respective roles and obligations under applicable Privacy Laws. For such Processing, the scope and roles of the parties shall be documented in the separate written agreement between Supplier and the Visa Client, in accordance with applicable Privacy Laws. For Processing under this Section 3.5, Visa does not act as a Controller or Processor for Supplier's direct Processing, except to the extent Visa separately Processes Personal Information for its own purposes under the Agreement. Supplier remains responsible for complying with Privacy Laws applicable to Supplier's Processing, including providing legally required notices, honoring applicable data subject rights, implementing appropriate data protection terms, and complying with any direct contractual obligations owed to the Visa Client.
- 3.6 **Independent Controller Activities of Supplier.** Supplier shall not Process Personal Information obtained from Visa or Processed on Visa's behalf as an independent Controller unless such Processing is expressly permitted by the Agreement, authorized by Visa in writing, documented in Annex 1, or required by applicable Privacy Laws. Where Supplier determines that Processing as an independent Controller is required by applicable Privacy Laws, Supplier shall notify Visa in writing prior to commencing such Processing. Where Supplier acts as an independent Controller, Supplier shall Process Personal Information only within the permitted, authorized, documented, or legally required scope; comply with applicable Privacy Laws; maintain protections no less protective than those required under this DPA for comparable Personal Information; and notify Visa without undue delay of any Data Breach involving Personal Information obtained from Visa, Processed on Visa's behalf, or otherwise relevant to Visa's obligations. Supplier remains a Processor (or Subprocessor, as applicable) for all other Processing of Personal Information under this DPA.
- 3.7 **Joint Controllership.** The Parties do not intend to act as joint Controllers under this DPA unless expressly agreed in writing or joint controllership is required by applicable Privacy Laws. If joint controllership applies, the Parties shall promptly execute a separate written arrangement allocating their respective responsibilities for compliance with applicable Privacy Laws. Further, Supplier shall not Process Personal Information as a joint Controller until notice of the joint Controller arrangement is made available to Data Subjects. Pending execution of such arrangement, each Party remains responsible for its own obligations under Privacy Laws for the Processing it undertakes.
- 3.8 **Documentation of Roles (Annex 1).** Annex 1 identifies the applicable role configuration(s) for the relevant engagement, use case, or Processing activity and may identify more than one configuration for different Processing activities. Supplier shall promptly notify Visa of any changes that may materially affect the role determinations documented in Annex 1.
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 or Processor (as the case may be) and Supplier shall comply with those obligations under Privacy Laws applicable to it as a Processor, Subprocessor, or independent Controller (as the case may be). Supplier agrees that it will not Process Personal Information or perform any of its obligations under the Agreement in such a way as to cause Visa to breach any of its obligations under Privacy Laws. Supplier shall promptly notify Visa if, in its opinion, the instructions given by Visa or its Affiliates for Processing violate any law. Supplier shall also promptly notify Visa of any circumstances that may prevent it or any Subprocessor from complying with their respective obligations under any applicable Privacy Law and/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" (PHI) as defined in the U.S. Health Information Portability and Accountability Act ("HIPAA"), Supplier and Visa agree that the

Visa Business Associate Agreement Terms are to be incorporated herein as required by HIPAA.

- 5.3 Privacy Notice:** If performance under the Agreement involves Supplier's collection of Personal Information on behalf of Visa or a Visa Client directly from individuals, Supplier shall provide the individuals with a clear and conspicuous privacy notice in the form and manner acceptable to Visa in Visa's sole and absolute discretion, which notice will either be (i) Visa's or its Affiliate's privacy notice, or (ii) Supplier's privacy notice, provided always 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 prior to publication.
- 5.4 Executive Order 14117 Compliance:** 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 shall limit access to the Personal Information to its Personnel that need to access such Personal Information to perform its obligations under the Agreement. Prior to allowing Personnel to Process such Personal Information, Supplier shall (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 from time to time. Supplier shall also monitor its Personnel for ongoing compliance with this DPA and apply appropriate disciplinary measures for individuals that fail to comply.
- 7. Data Security.** Supplier shall 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 shall include, and comply with, all measures identified in the Visa Supplier Security Standards, comply with applicable Privacy Laws, reflect industry best practices, and include any additional measures that are specified in the Agreement.
- 8. Automated Decision-Making.** Where Supplier uses any automated decision-making systems, algorithms, or artificial intelligence in connection with the Processing of Personal Information under this Agreement, Supplier shall have an ongoing obligation to: (i) ensure that appropriate human oversight and intervention mechanisms are in place; and (ii) comply with all applicable Privacy Laws relating to automated decision-making, including any requirements for transparency, explainability, and/or human review.
- 9. Transfers of Personal Information.**
- 9.1** For any Transfer, Parties hereby rely on the first of the following mechanisms that lawfully permits such Transfer: (a) an adequacy decision or similar determination issued by a competent supervisory authority; (b) binding corporate rules applicable to the transferring Party, to the extent recognized under applicable Privacy Laws; or, failing the foregoing, (c) the provisions of Annex 2.
- 9.2** Where none of the foregoing mechanisms lawfully permit the Transfer, the Parties shall cooperate in good faith to implement such appropriate transfer mechanism(s) as required under applicable

Privacy Laws.

- 9.3 Supplier, in respect of transfers contemplated under the Agreement for which it is reasonably aware, shall take all steps reasonably necessary to facilitate lawful Transfers to Visa under this Agreement, including without limitation applying appropriate safeguards, obtaining necessary and valid consents, completing any registrations, notifications, security assessments or certifications, and obtaining regulatory approvals as may be required of Supplier under applicable Privacy Laws.
- 9.4 Visa hereby approves the Transfers described in the Agreement (including the Annexes to this DPA). Supplier hereby undertakes that any Transfers of Personal Information made shall be carried out in accordance with the requirements of the relevant Privacy Laws. Except for Transfers contemplated under this Agreement (including the Annexes to this DPA), Supplier shall not make any other Transfers (each a “**proposed Transfer**”) 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 (Subprocessors). Supplier shall notify Visa prior to any proposed Transfer of Personal Information in addition to those described in Annex 1, 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 shall not undertake any proposed Transfers until such objections or requirements (as applicable) have been addressed to Visa’s reasonable satisfaction.

10. Subprocessors.

- 10.1 Supplier shall provide Visa with a list of all Subprocessors (the “**Subprocessor List**”) as at the date of the Agreement in the form set out in Annex 1 below. Visa hereby authorizes Supplier to engage the Subprocessors listed in Annex 1 subject to the terms of this Agreement. Supplier shall not authorize any additional Subprocessors to Process Personal Information without Visa’s prior consent as described in this Section. For each of its Subprocessors, Supplier shall:
- (A) Conduct adequate due diligence on the Subprocessor 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 Subprocessor that includes terms equivalent to those contained in this DPA and the Agreement (offering the same or higher level of protection for Personal Information) and provides that the Subprocessor’s right to Process Personal Information may be terminated by Supplier immediately on expiry or termination of the Agreement for whatever reason; and
 - (C) Remain 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 shall notify Visa thirty (30) days prior to any proposed addition of a new Subprocessor. Visa will evaluate proposed new Subprocessors and notify Supplier within thirty (30) days (i) if the addition is approved or (ii) of any objection. In the event that Visa does not object to a proposed Subprocessor within thirty (30) days after receiving notice from Supplier about the Subprocessor, the new Subprocessor will be deemed approved by Visa. Supplier shall not allow such Subprocessor to access any Personal Information until the objection is addressed to Visa’s reasonable satisfaction.
- 10.3 Upon request, Supplier shall provide Visa with a most-current copy of the Subprocessor List along with copies of the due diligence it conducted and its agreements with its Subprocessors (which may be redacted to remove confidential commercial information not relevant to compliance with this DPA).
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 shall (unless prohibited by law) promptly notify Visa. If the Third-Party Request is not legally valid and binding, Supplier shall not respond to it. If a Third-Party Request is legally valid and binding, Supplier shall 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 shall make commercially reasonable efforts to prevent and limit any such disclosure and to otherwise preserve the confidentiality of Personal Information. Supplier shall also cooperate with Visa and Visa’s Affiliates with

respect to any action taken with respect to such Third-Party Request, including obtaining an appropriate protective order or other reliable assurance that confidential treatment will be accorded to Personal Information. In all cases, Supplier shall 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 shall promptly notify Visa of any Data Subject Requests by sending an email to privacy@visa.com. Without limiting the foregoing, unless otherwise agreed (such as for handling of requests contemplated by the Agreement), Visa or its Affiliates will handle Data Subject Requests, and Supplier shall 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 shall 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 shall also provide a copy to Visa of all Personal Information and any relevant information that it discloses.
13. **Data Protection Impact or Risk Assessments and Prior Consultation with Regulator.** As may be required by Privacy Laws, Supplier shall 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 (or its Subprocessors, as applicable). In particular, to the extent that the Services entail any High Risk Processing Activities, Supplier will conduct risk assessments as required by the applicable Privacy Laws, and it will provide Visa with all information and documentation reasonably necessary to enable Visa to accurately identify and address risks associated with any High Risk Processing Activities and to comply with its own obligations under the Privacy Laws.
14. **Return, Deletion and Retention.** When Supplier ceases to perform Services for Visa and/or upon expiration of the retention period(s) identified in Annex 1 (and at any other time, upon request), Supplier shall either (i) purge, delete and destroy Personal Information or, upon Visa's request, (ii) return Personal Information (and all media containing copies of Personal Information) to Visa prior to such deletion. Electronic media containing Personal Information shall be disposed of in a manner that renders Personal Information unrecoverable. If Supplier is required by Applicable Law to retain any Personal Information, Supplier shall (i) document such retention period in Annex 1, (ii) ensure the continued confidentiality and security of the Personal Information, (iii) securely delete or destroy Personal Information when the legal retention period has expired, and (iv) not actively Process Personal Information other than as needed to comply with law.
15. **Consent Management.** Where Supplier is required to obtain consent from individuals for any Processing of Personal Information under this Agreement (including consent for collection, use, disclosure, or Transfer), Supplier shall: (i) obtain such consent in a manner that complies with all applicable Privacy Laws, including any requirements as to form, content, timing, and revocability; (ii) maintain accurate records of all consents obtained, including the date, method, and scope of consent; (iii) provide Visa with access to such consent records upon request; (iv) promptly notify Visa of any withdrawal of consent by an individual; and (v) implement appropriate mechanisms to give effect to any withdrawal of consent. Supplier shall not rely on deemed, implied, or bundled consent where applicable Privacy Laws require express or specific consent.
16. **Data Breaches.** In accordance with the Security Event provision of the Security Standards Exhibit, Supplier shall promptly and thoroughly investigate all alleged or suspected instances of a Data Breach involving Personal Information and shall report (in the form and manner, and according to the specified timelines under the Security Events provision) any event reasonably believed to constitute a Data Breach involving Personal Information to Visa.
17. **Data Localization.** Without limiting any other provision under this DPA, Supplier shall: (i) promptly notify Visa of any Data localization Requirements applicable to the Personal Information; (ii) comply with all Data Localization Requirements at Supplier's cost; (iii) provide Visa with reasonable assistance in conducting any localization assessments or implementing localization measures required by Privacy Laws; and (iv) not Transfer Personal Information from any jurisdiction that imposes Data Localization Requirements unless such Transfer is expressly permitted under the applicable Privacy Laws and approved by Visa in writing.
18. **Third-Party Beneficiaries.** Supplier hereby agrees and acknowledges 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.

19. **Conflicts and Consideration.** This DPA supersedes any conflicting provision of the Agreement related to the Processing of Personal Information. A violation of this DPA shall be deemed to constitute a material breach of the Agreement.
20. **Term and Survival.** The obligations of Supplier under this DPA shall 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 2: CROSS BORDER TRANSFER ADDENDUM

This Cross-Border Transfer Addendum (**Transfer Addendum**) applies pursuant to Section 10 of the DPA to all Transfers which take place under the Agreement. The allocation of data protection roles (including whether Visa acts as Controller or Processor) shall be as specified in the DPA.

1. Definitions and interpretation

1.1 The following definitions apply in addition to the terms of the Agreement, including the DPA:

- (A) **“Data Exporter”** means the party who initiates the transfer (by way of a Transfer) of relevant Personal Information to a Data Importer;
- (B) **“Data Importer”** means the party which, acting either as a Processor or Controller, receives (by way of a Transfer) relevant Personal Information from a Data Exporter;
- (C) **“Supervisory Authority”** means any regulatory or competent authority responsible for the enforcement of Privacy Laws;
- (D) **“Transfer Mechanism”** means the transfer mechanism specified in section 5 for a particular jurisdiction, which may include (without limitation) standard contractual clauses, binding corporate rules, certifications, codes of conduct, or any other mechanism approved by the relevant Supervisory Authority.

2. Transfers

- 2.1 The Privacy Laws in certain jurisdictions where Transfers between the parties take place may require specific Transfer Mechanisms to be entered into between the parties. The relevant provisions of the Agreement and this Transfer Addendum shall be interpreted in accordance with any relevant Transfer Mechanism(s) set out in section 5 as applicable to a Transfer originating from a jurisdiction specified in section 5.
- 2.2 The Parties acknowledge that, in the context of a Transfer, a party may be either a Data Exporter or Data Importer depending on the nature of the Transfers which take place under the Agreement.
- 2.3 The Transfer Mechanisms set out in section 5 below shall come into effect on the commencement of the Transfer.

3. Order of Precedence

- 3.1 In the event of any conflict, ambiguity or inconsistency relating to Transfers, this Transfer Addendum and any other agreement(s) between the parties, the following order of precedence shall apply:
 - (A) The mandatory provisions of any applicable Transfer Mechanism (first);
 - (B) This Transfer Addendum (second);
 - (C) The DPA (third); and

(D) The Agreement (last).

4. General

- 4.1 Save where a Transfer Mechanism specifies a different governing law for the purposes of that mechanism, this Transfer Addendum shall be governed by and construed in accordance with the governing law specified in the Agreement.
- 4.2 Visa may vary the terms of this Transfer Addendum to reflect changes required by applicable Privacy Laws, to incorporate new or updated Transfer Mechanisms or to improve the language or functionality of this Transfer Addendum, provided that such updates do not materially reduce the level of protection afforded to Personal Information.
- 4.3 If any provision of this Transfer Addendum is held to be invalid or unenforceable, the remaining provisions shall continue in full force and effect.

5. Transfer Mechanisms

Country / Region of Origin	Special Terms
5.1 European Union (EU)	Where a Transfer is subject to the EU GDPR, Supplier as Data Exporter and Visa/its affiliate each as Data Importer hereby enter into Module 1 or Module 2, as relevant, of the EU SCCs which are incorporated into this Transfer Addendum by reference, and, in: Clause 7, the optional clause will apply; Clause 9 of Module 2, option 2 will apply, and the time period for prior notice of Subprocessor changes will be in accordance with the notification process set out in the Agreement; Clause 11, the optional redress language will not apply; Clause 13, the supervisory authority shall be the Irish Data Protection Commission; Clause 17, option 1 will apply and the Member State shall be Ireland; Clause 18, disputes shall be resolved before the courts of Ireland; Annexes 1, 2 and 3 will be deemed to be pre-populated with the relevant sections of the Agreement. Where a Transfer is subject to the EU GDPR, Visa/its affiliates as Data Exporter and Supplier as Data Importer hereby enter into Module 2 or Module 3, as relevant, of the EU SCCs which are incorporated into this Transfer Addendum by reference, and, in: Clause 7, the optional clause will apply; Clause 9, option 1 will apply, and the time period for prior notice of Subprocessor changes will be in accordance with the notification process set out in the Agreement; Clause 11, the optional redress language will not apply; Clause 13, the supervisory authority shall be the Irish Data Protection Commission; Clause 17, option 1 will apply and the Member State shall be Ireland; Clause 18, disputes shall be resolved before the courts of Ireland; Annexes 1, 2 and 3 will be deemed to be pre-populated with the relevant sections of the Agreement.
5.2 United Kingdom (UK)	In respect of any Transfer which is subject to UK GDPR, the EU SCCs (as incorporated by reference pursuant to 5.1 above) shall be read in accordance with, and deemed amended by, the provisions of Part 2 (Mandatory Clauses) of the UK SCCs, and the Parties confirm that the information required for the purposes of Part 1 (Tables) of the UK SCCs is as set out in the Agreement.

Country / Region of Origin	Special Terms
5.3 Switzerland	Where a Transfer is subject to the Swiss Federal Data Protection Act ("FADP"), the EU SCCs shall be amended as follows: (A) References to GDPR in the EU SCCs shall be understood as references to the FADP insofar as the data transfers are subject to the FADP. (B) Competent supervisory authority (Clause 13 of the EU SCCs): The Swiss Federal Data Protection and Information Commissioner (FDPIC) shall act as the competent supervisory authority. (C) Governing law (Clause 17 of the EU SCCs): For contractual claims regarding data transfers pursuant to the FADP, these clauses shall be governed by the law of Ireland. (D) Choice of forum and jurisdiction (Clause 18.a/b of the EU SCCs): For actions concerning data transfers pursuant to the FADP, any dispute arising from these clauses shall be resolved by the courts of Ireland. (E) Data subject jurisdiction (Clause 18c of the EU SCCs): The term "Member State" shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of pursuing their rights at their place of habitual residence (Switzerland) in accordance with clause 18c of the EU SCCs. Accordingly, data subjects with their place of habitual residence in Switzerland may also bring legal proceedings before the competent courts in Switzerland.
5.4 Mainland China	Part A: Definitions and Applicability Mainland China: the People's Republic of China (for the purpose of this DPA only, excluding Hong Kong SAR, Macau SAR and Taiwan). China SCCs: the China Standard Contract for Overseas Transfer of Personal Information as issued by the Cyberspace Administration of China (CAC). PIPL: the China Personal Information Protection Law. Where a Transfer is subject to applicable Chinese laws and regulations, including, without limitation, the PIPL, the following provisions shall apply. This section (Parts A-D) applies only to Personal Information that the Data Importer receives or accesses from a Data Exporter located in Mainland China. Part B: Obligations of the Data Exporter The Data Exporter located in Mainland China shall: (A) Ensure that the Transfer of Personal Information to the Data Importer complies with applicable Chinese laws and regulations on cross-border transfer, and that all necessary approvals, filings, or certification procedures have been completed. (B) Conduct or ensure that its partner(s) conduct (where such partner is the data controller), a Personal Information Protection Impact Assessment ("PIPIA") in accordance with applicable Chinese laws and regulations for the Transfer of Personal Information to the Data Importer, and the processing activities shall

Country / Region of Origin	Special Terms
	be recorded. The retention period for the relevant PIPIA assessment and records shall also comply with the requirements of applicable Chinese laws and regulations. Part C: Obligations of the Data Importer The Data Importer shall: (A) Cooperate with the Data Exporter or its partner(s) (where such partner is the data controller) in completing necessary approvals, filings, or certification procedures for the Transfer of Personal Information. (B) Cooperate with the Data Exporter in conducting PIPIA and Personal Information Protection Compliance Assessment (“PIPCA”) for the Transfer, if required. Part D: China SCCs (where applicable) Where and to the extent the China SCCs are required under applicable Chinese laws and regulations for the Transfer, the Parties shall cooperate with each other to enter into the China SCCs.
5.5 Thailand	(A) Where a Transfer is subject to Thailand Personal Data Protection Act B.E. 2562 (2019) (PDPA), Visa/its affiliate(s) and Supplier, each as Data Exporter or Data Importer (as the case may be), hereby enter into the relevant Module(s) of the EU SCCs (as incorporated by reference pursuant to 5.1 above) to the extent such mechanism is recognised or permissible under the PDPA, subject to the following amendments: (B) References to GDPR in the EU SCCs shall be understood as references to the PDPA insofar as the data transfers are subject to the PDPA. (C) Competent supervisory authority (Clause 13 of the EU SCCs): The Office of the Personal Data Protection Committee of Thailand shall act as the competent supervisory authority. (D) Governing law (Clause 17 of the EU SCCs): For contractual claims regarding data transfers pursuant to the PDPA, these clauses shall be governed by the law of Singapore. (E) Choice of forum and jurisdiction (Clause 18.a/b of the EU SCCs): For actions concerning data transfers pursuant to the PDPA, any dispute arising from these clauses shall be referred to and finally resolved by arbitration administered by the International Chamber of Commerce (“ICC”) in accordance with the Rules of Arbitration of the ICC for the time being in force, which rules are deemed to be incorporated by reference in this clause. The seat of the arbitration shall be Singapore. The Tribunal shall consist of one (1) arbitrator. The language of the arbitration shall be English. (F) Data subject jurisdiction (Clause 18c of the EU SCCs): The term "Member State" shall not be interpreted in such a way as to exclude data subjects in Thailand from the possibility of pursuing their rights at their place of habitual residence (Thailand) in accordance with clause 18c of the EU SCCs. Accordingly, data subjects with their place of habitual residence in Thailand may also bring legal proceedings before the competent courts in Thailand.

Country / Region of Origin	Special Terms
5.6 Vietnam	Where a Transfer is subject to the laws of Vietnam, the Data Exporter shall ensure that it has obtained prior consent from the relevant data subjects, unless a consent-exemption applies, and shall ensure compliance with applicable laws, including obtaining any prior approval (if applicable) required for cross-border transfers from Vietnam. The parties shall comply with requirements regarding data protection impact assessments to the extent required with respect to the relevant Transfer.
5.7 Singapore	Where a Transfer (by a Data Exporter located in Singapore) is subject to the laws of Singapore, the Data Importer (located outside of Singapore) shall provide a standard of protection to Personal Information so transferred that is at least comparable to the protection under the Singapore Personal Data Protection Act 2012.
5.8 India	Where a Transfer is subject to the Digital Personal Data Protection Act (“DPDPA”) of India: (A) Data Exporter confirms and undertakes that: (i) any Transfer of Personal Information to a Data Importer outside the territory of India complies with the DPDPA; and (ii) no restrictions notified by the Central Government apply to the relevant Transfer or Transfer destination(s). The Data Exporter further confirms that, at the time of each Transfer, it (or the Data Fiduciary on whose behalf it acts) has a valid consent or a valid legitimate use, as applicable, under the DPDPA and its implementing rules, as a lawful basis for the processing and transfer of the relevant Personal Information; (B) Additionally: (i) the Data Exporter shall comply with any applicable requirements specified by the Central Government in connection with making Personal Information available to any foreign State, or to any person or entity under the control of, or any agency of, such a State; (C) (ii) where Data Exporter is a Significant Data Fiduciary (or is included in a class of Data Fiduciaries notified as such), Data Exporter shall ensure compliance with any applicable data localisation requirements, including ensuring that any conditions applicable to any cross border data flows specified by the Central Government by notification are complied with and restricted categories of Personal Information as specified by the Central Government and the traffic data pertaining to its flow are not transferred outside the territory of India; and (iii) Data Exporter shall comply with any other applicable law for the time being in force in India that provides for a higher degree of protection for, or restriction on, transfer of Personal Information outside India (including, without limitation, any applicable sectoral data localisation requirements imposed by the Reserve Bank of India, the Securities and Exchange Board of India, the Insurance Regulatory and Development Authority of India, and/or any other regulatory authority); and (D) The Parties shall review any requirement to implement reasonable and appropriate measures as may be necessary for any Transfer or localisation-related requirements or restrictions imposed by the Central Government or under Applicable Data Protection Law. In this Section 5.8, references to “Data Fiduciary” and “Significant Data Fiduciary” shall have the meanings respectively ascribed to them under the DPDPA and its implementing rules.

Country / Region of Origin	Special Terms
5.9 United Arab Emirates (UAE Federal)	Where a Transfer is subject to the United Arab Emirates (UAE) Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data (PDPL) the EU SCCs shall apply <i>mutatis mutandis</i> and be amended to comply with all PDPL requirements for such Transfers. Without prejudice to the generality of the foregoing, the following amendments to the EU SCCs shall apply: (A) The "competent supervisory authority" and "supervisory authority" shall be replaced with the "applicable UAE supervisory authority". (B) References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are all replaced by "the UAE's Personal Data Protection Law". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of the UAE's Personal Data Protection Law. (C) References to Regulation (EU) 2018/1725 shall be omitted. (D) References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "United Arab Emirates". (E) The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module 1 is replaced with "Clause 11(c)(i)". (F) Clause 13(a) and Part C of Annex I are not used and shall be omitted. (G) Clause 16(e)(i) is replaced with: "a UAE supervisory authority makes regulations that cover the transfer of personal data to which these Clauses apply;" (H) Clause 17 is replaced with: "These Clauses are governed by the federal laws of the United Arab Emirates." (I) Clause 18 is replaced with: "Any dispute arising from these Clauses shall be resolved by the courts of the United Arab Emirates. The Parties agree to submit themselves to the jurisdiction of such courts." (J) The footnotes shall be removed.
5.10 Saudi Arabia	Where a Transfer is subject to the Kingdom of Saudi Arabia Personal Data Protection Law (issued pursuant to Royal Decree No. (M/19) dated 09/02/1443 (KSA PDPL), Supplier as Data Exporter and Visa/its affiliate each as Data Importer hereby enter into Template 1 or Template 2, as relevant, of the Kingdom of Saudi Arabia Standard Contractual Clauses as issued by the Saudi Data and AI Authority and set out at "https://sdaia.gov.sa/Documents/StandardContractualClausesForPersonalDataTransferEN.pdf" as amended from time to time (KSA SCCs), which are incorporated into this Transfer Addendum by reference, and, Appendices 1, 2 and 3 of the KSA SCCs will be deemed to be pre-populated with the relevant sections of the Agreement. Where a Transfer is subject to the KSA PDPL, Visa/its affiliates as Data Exporter and Supplier as Data Importer hereby enter into Template 2 or Template 3, as relevant, of

Country / Region of Origin	Special Terms
	the KSA SCCs which are incorporated into this Transfer Addendum by reference, and, Appendices 1, 2 and 3 of the KSA SCCs will be deemed to be pre-populated with the relevant sections of the Agreement.
5.11 Argentina, Colombia, Ecuador, Peru, Uruguay, Panama and other LAC countries where IDPN SCCs are formally adopted.	I. Where a Transfer is subject to the Argentine Data Protection Law No. 25.326, the Colombian Data Privacy Laws No. 158, the Ecuador Personal Data Protection Organic Law, the Panama Data Protection Law N° 81, the Peru Personal Data Protection Law N° 29733, the Uruguayan Data Protection Law No. 18,331, all of them as amended and jointly with their regulations and complementary rules applicable to the protection of personal data, the Supplier/Provider as Data Exporter and Visa/its Affiliate as Data Importer, or vice versa as the case may be, hereby enter into Module 1 Controller to Controller or Module 2 Controller to Processor, as relevant, of the Ibero-American Data Protection Network and set out at annex-model-contractual-clauses-en.pdf (“IDPN SCCs”) as adopted by the Argentinean Agency for Access to the Public Information pursuant to Resolution 198/2023, the Ecuadorian Personal Data Protection Superintendence pursuant to Resolution SPDP-SPD-2026-0004-R, the Panama National Authority for Transparency and Access to Information through Resolution No. ANTAI-DG-003-2026, the Peru Data Protection National Authority pursuant to Directorial Resolution N.° 0074-2022-JUS/DGTAIPD, and the Uruguay Regulatory and Control Unit of Personal Data via Resolution No. 50/022, which are incorporated into this Transfer Addendum by reference, and, in: (A) Clause 5 the optional clause will not apply; (B) Clause 7.1. of Module 2 Controller to Processor, option 2 will apply and the time period for prior notice of Subprocessor changes will be in accordance with the notification process set out in the Agreement. (C) Clause 8 of Module 1 and Clause 9 of Module 2, the optional redress language will not apply; (D) For the purposes of Clause 6.9 (onward transfers), the data importer may only effect onward transfers in accordance with the conditions set out therein and in compliance with the requirements set out in the applicable Privacy Laws. (E) The applicable law for the purposes of Clause 13 shall be the law of the country of the data exporter. (F) For the purposes of Clause 14, disputes shall be resolved before the courts of (G) the jurisdiction of the data exporter, provided that data subjects may also exercise actions before the courts of their habitual residence; (H) The competent supervisory authority for the purposes of Clause 10 shall be the one of the country of the data exporter. (I) Annexes A, B, C, and D shall be deemed pre-populated with the relevant information set out in the Agreement and this Transfer Addendum; For the avoidance of doubt, these IDPN SCCs shall apply regardless of whether Supplier or Visa acts as Data Exporter.

Country / Region of Origin	Special Terms
	II. Once and if, the IDPN SCCs are formally adopted by any other Data Protection Authority across LAC jurisdictions, and as of the date of its adoption, where a Transfer is subject to such jurisdiction Privacy Laws, the Supplier/Provider as Data Exporter and Visa/its Affiliate as Data Importer, or vice versa as the case may be, agree that Module 1 Controller to Controller or Module 2 Controller to Processor, as relevant, of the IDPN will be automatically incorporated into this Transfer Addendum by reference as adopted by the relevant supervisory authority and pursuant to the adoption regulation. Unless otherwise specified by the relevant LAC jurisdiction Data Privacy Laws, sections a. to h. above will be applicable.
5.12 Brazil	Where a Transfer is subject to the LGPD, Supplier as Data Exporter and Visa/its affiliate each as Data Importer hereby enter into the standard contractual clauses published in Annex II of Resolution CD/ANPD No. 19/2024 as set out in regulation-on-international-transfer-of-personal-data.pdf (the “ANPD SCCs”), which are incorporated into this Transfer Addendum by reference, as follows: • Clause 1.1: The Parties are identified in the Agreement. • Clause 2.1: The description of the international transfer is set out in the Agreement. • Clause 3: Option B shall apply, and the conditions of onward transfer (Main Purposes of the Transfer, Categories of Personal Data Transferred; Period of Data Storage; and Other Information Applicable to Onward Transfers) are set out in the Agreement. • Clause 4: Option A shall apply, and items a, b, and c shall be the responsibility of the Exporter. • Section III: Details of security measures are set forth in the Agreement. Where a Transfer is subject to the LGPD, Visa/its affiliates as Data Exporter and independent controller and Provider/Supplier as Data Importer, hereby enter into the standard contractual clauses published in Annex II of Brazilian SCCs, which are incorporated into this Transfer Addendum by reference, as follows: • Clause 1.1: The Parties are identified in the Agreement. • Clause 2.1: The description of the international transfer is set out in the Agreement. • Clause 3: Option B shall apply, and the conditions of onward transfer are set out in the Agreement. • Clause 4: Option A shall apply, and items a, b, and c shall be the responsibility of the Exporter. • Section III: Details of security measures are set forth in the Agreement. Where a Transfer is subject to the LGPD, Visa/its affiliates as Data Exporter and Provider as Data Importer, where Visa/its affiliates act as processor of data, hereby enter into the standard contractual clauses published in Annex II of Brazilian SCCs, which are incorporated into this Transfer Addendum by reference, as follows: • Clause 1.1: The Parties are identified in the Agreement. • Clause 2.1: The description of the international transfer is set out in the

Country / Region of Origin	Special Terms
	Agreement. • Clause 3: Option B shall apply, and the conditions of onward transfer are set out in the Agreement. • Clause 4: Option A shall apply, and items a, b, and c shall be the responsibility of the Importer. Section III: Details of security measures are set forth in the Agreement. Where the Transfer is made between Provider and a subprocessor, Visa hereby authorizes Provider to enter into the Brazilian SCCs with any approved Sub-processor for and on its behalf (or, where applicable, on behalf of the relevant Visa corporate customer).
5.13 Canada	1. Applicable law: If the Transfer is subject to the laws of Canada, the parties shall ensure such a Transfer is made in compliance with the relevant provisions of the applicable Canadian laws, including the <i>Personal Information Protection and Electronic Documents Act</i> and substantially similar provincial statutes. 2. Condition for transfers: Transfers may only take place where: (a) the destination country provides an adequate level of protection; and (b) appropriate contractual or equivalent safeguards are in place. 3. Privacy Impact Assessment: Each party shall complete and document, where legally required, a privacy impact assessment to confirm that the Personal Information subject to the Transfer is awarded protections at least equivalent to the protections awarded by applicable Canadian Privacy Laws. 4. Controller-to-Processor Transfers: In the context of any Controller-to-Processor Transfers, the party acting in its capacity as processor shall assume the following obligations (where required by applicable Privacy Laws): (A) implement appropriate technical and organizational measures proportionate to risks, including measures for encryption, access control, logging and monitoring, resilience, incident response and secure deletion to protect the confidentiality of the Personal Information communicated, and shall regularly test, assess and evaluate their effectiveness. (B) restrict the use and disclosure of the Personal Information communicated to what is strictly required for the provision of services. (C) at the end of the provision of services, at the controller's choice, delete or return all transferred Personal Information and delete existing copies unless retention is required by binding law notified to controller; where deletion is chosen, the processor shall securely and irreversibly delete data and certify completion. (D) notify the controller without delay of any violation or attempted violation by any person of any obligation concerning the confidentiality of the Personal Information communicated. (E) make available to the controller all information necessary to demonstrate compliance with applicable Canadian Privacy Laws and shall allow for and contribute to audits, including inspections, conducted by the controller or an auditor mandated by the controller, on reasonable notice and at reasonable intervals.

Country / Region of Origin	Special Terms
5.14 Israel	Where a Transfer is subject to the Israeli Protection of Privacy Law, 1982, and the regulations promulgated thereunder, including the Protection of Privacy Regulations (Data Security), 2017 (the “Data Security Regulations”), and the Protection of Privacy Regulations (Transfer of Data to Databases Outside the Borders of the State), 2001 (the “Data Transfer Regulations”) (collectively, the “PPL”), the Data Exporter confirms and undertakes that any Transfer to a Data Importer outside the territory of the State of Israel complies with the PPL. Data Importer undertakings. The Data Importer shall ensure that any Personal Data shall be processed in compliance with Privacy Laws including the PPL. The Data Importer shall not transfer any Personal Data to a third party on its behalf unless the Data Exporter authorized (including by general authorization) such transfer in writing and ensured that the third party is bound by obligations that provide a level of protection for the Personal Data that is no less protective than that set out in the Agreement. EU SCCs. For Transfers subject to the PPL, the EU Standard Contractual Clauses shall apply, with the following modifications: (a) the terms “General Data Protection Regulation” or “Regulation (EU) 2016/679,” as used in the EU Standard Contractual Clauses, shall be deemed to refer to the PPL; (b) references to specific sections or provisions of the GDPR in the EU Standard Contractual Clauses shall be read as references to the corresponding sections or provisions of the PPL; (c) Clause 13 of the EU Standard Contractual Clauses shall be deemed to provide that the Israeli Privacy Protection Authority (the “PPA”) shall have authority over data transfers governed by the PPL; (d) the term “EU Member State,” as used in the EU Standard Contractual Clauses, shall not be interpreted in a manner that excludes Data Subjects in the State of Israel from exercising their rights in their place of usual residence in accordance with Clause 18(c) of the EU Standard Contractual Clauses; and (e) Annexes I and II to the Addendum shall apply to Transfers. Data Security. In relation to a Data Breach notification, the Data Importer shall notify the Data Exporter immediately after becoming aware of a Severe Security Incident (as defined under the PPL) related to Personal Data subject to a Transfer. The Data Importer shall to the extent necessary provide the Data Exporter with an annual report on the security measures implemented to protect the security and integrity of the Personal Data. Cooperation. The Data Importer shall reasonably cooperate with the Data Exporter in the event of PPA enforcement actions, queries, or investigations, and shall reasonably cooperate with the Data Exporter to ensure the implementation of measures required under the PPL.
5.15 Turkey	1. Applicable law: Where a Transfer is subject to the Personal Data Protection Law No. 6698 (“DPL”), the Parties shall ensure that such transfer is made in compliance with the DPL and the Regulation on the Procedures and Principles for Cross-Border Transfers of Personal Data published by the Turkish Data Protection Authority (“DPA”) on 10 July 2024 (“Regulation”). 2. Condition for transfers: Transfers may only take place where one of the transfer mechanisms set out in Article 9 of the DPL is in place. The parties agree that Standard Clauses (“Turkish SCCs”) published by the DPA shall serve as the applicable transfer mechanism and shall enter into the applicable transfer mechanism in the event of a Transfer subject to the DPL.

ANNEX 3: U.S. STATE LAW COMPLIANCE REQUIREMENTS

As used in this Annex, the following terms have the meanings set forth in (collectively) the CCPA (as amended), all implementing regulations, as and when effective, and any other 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 provided that the retention, use, or disclosure is reasonably necessary and proportionate for the Business Purposes identified in Annex 1 to this DPA.
 - 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 Will cooperate with Visa in the completion of any cybersecurity audits and/or risk assessments required by a CPA, including making available to Visa or Visa’s auditor all relevant information requested to complete such cybersecurity audit and/or risk assessment that is in the Supplier’s possession, custody, or control, and will not misrepresent any fact that Visa or Visa’s auditor deems relevant to Visa’s cybersecurity audit and/or risk assessment.

- 1.11 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.

ANNEX 4: ADDITIONAL PROTECTIONS FOR EUROPEAN PERSONAL DATA

The contractual protections set out in this Annex 4 shall apply only to Transfers of European Personal Data subject to either the GDPR and/or UK GDPR.

1. **Definitions.** For the purposes of this Annex 4 (Additional Protections for European Personal Data), the following capitalized terms have the meanings provided below. Capitalized terms not defined below shall have the meaning set forth in the Agreement.
 - 1.1 **"Public Body"** means any local, regional, state, national or federal law enforcement authority, regulator, government department, agency or court in any Third Country.
 - 1.2 **"Third Country"** means a country which is not a Member State of the EEA or the UK, and which does not benefit from an adequacy decision under Article 45 of the GDPR or UK GDPR (with respect to Transfers subject to the GDPR or UK GDPR respectively).
 - 1.3 **"Third-Party Request"** means any criminal, civil, or administrative subpoena, mandatory request, order, demand, warrant, or any other document requesting or purporting to compel the production of European Personal Data, including but not limited to subpoenas, warrants and orders authorized under local, regional, state, national or and federal laws or regulations or any other laws applicable to the Supplier or its Affiliates in any Third Country.
2. The commitments given in this Annex 4 are in each case without prejudice to the commitments given by Supplier in the DPA, the Agreement and in the EEA Standard Contractual Clauses and UK SCCs (as applicable), as well as those under applicable Privacy Laws.
3. Supplier warrants that neither it nor its Affiliates have taken any steps to facilitate access to European Personal Data (including systems on which European Personal Data is Processed) by any Public Body, including, without limitation, by creating back-doors or similar programming that provide a mechanism for a Public Body to access European Personal Data or changing its business processes with the express intention of facilitating access to European Personal Data. Supplier certifies that neither it nor its Affiliates are subject to laws that would require it or its Affiliates to take any of the steps referred to this Section 3.
4. If Supplier or its Affiliates receive a Third-Party Request, Supplier shall attempt to redirect the Public Body issuing such Third-Party Request to request that European Personal Data directly from Visa. If this is not possible, Supplier shall permit Visa to respond to the Third-Party Request directly, unless Supplier is legally prohibited from doing so. Any disclosure made by Supplier or its Affiliates in response to a Third-Party Request shall be made in compliance with Privacy Laws (including the GDPR and/or UK GDPR, as applicable) and the EEA Standard Contractual Clauses and/or UK SCCs (as applicable) to the greatest extent possible.
5. Supplier shall implement and maintain appropriate procedures for the assessment and handling of Third-Party Requests, which shall be aligned to the requirements of Privacy Laws and this DPA, and provide training on those procedures to its Personnel.
6. Supplier shall maintain accurate and up-to-date written records of all Third-Party Requests. Upon request, Supplier agrees to provide Visa with a "transparency report" regarding all requests for access to Visa Personal Information (whether European Personal Data or otherwise) received from Public Bodies over a specified period. The report should not disclose the identity of any other client or customer of Supplier, but must detail the type of information requested and the legal power under which the request was made.
7. Supplier shall ensure that its Data Protection Officer has oversight of Supplier's approach to Transfers and

is involved in determining the response to any Third-Party Request for European Personal Data.

8. Upon request, Supplier agrees to cooperate with and assist data subjects seeking to exercise their rights or obtain effective redress in a Third Country in relation to a Transfer.