**VISA CONSUMER AUTHENTICATION SERVICE**
**DATA PROCESSING AGREEMENT**

**This Data Processing Agreement** ("DPA") is an agreement between you and the entity you represent ("Customer" or "you"), on the one hand, and CardinalCommerce Corporation and/or any other applicable affiliated CardinalCommerce contracting entity(ies) ("Cardinal" or "CardinalCommerce"), on the other hand. It forms part of any written or electronic agreement between you and Cardinal under which Cardinal Processes Personal Information on your behalf (each, an "Agreement"), except with respect to any Agreement under which you and Cardinal have entered data processing terms that address the subject matter hereof. Each of Cardinal and Customer may be referred to herein as a "party" and collectively as the "parties."

1 **Processing of Customer Personal Information**. The parties acknowledge and agree that Cardinal will Process certain Personal Information ("Customer Personal Information") to carry out the authentication service (the "Service") as detailed in the table appended to this DPA at Exhibit 1. To the extent necessary to enable each party to comply with its obligations under Applicable Data Protection Law, each party further agrees to comply with any required provisions of Schedule A: General Data Protection Regulation, if applicable, and that if GDPR applies, Cardinal is acting as joint controllers with you.

2 **Compliance with Law**. Cardinal, in its provision of the Service to Customer, and Customer, in its use of the Service, shall Process Customer Personal Information in accordance with Applicable Data Protection Law.

3 **Notice**. Customer shall provide its Data Subjects, as defined below, with all privacy notices, information and any necessary choices and shall obtain any necessary consents to enable Cardinal to comply with Applicable Data Protection Law.

4 **Data Subject Rights**. The parties agree that to the extent applicable, that Customer shall be the designated point of contact for the Data Subject with respect to Data Subject Rights requests for Services, and Cardinal shall reasonably cooperate with and assist Customer in the execution and fulfilment of its obligations under Applicable Data Protection Laws in relation to such requests. Cardinal will not respond to a Data Subject without Customer's prior approval.

5 **Reasonable Assistance**. With respect to the Services, each party shall assist the other party as reasonably required, in meeting any regulatory obligations in relation to data security, notification of a Security Breach, and data protection impact assessments for the Services.

6 **Supervisory Authority**. The parties shall without undue delay notify each other upon receipt of any correspondence from a Supervisory Authority in respect of the Services where and to the extent permitted by applicable law.

7 **Security of Processing and PCI Compliance**. Each party shall be responsible for ensuring adequate security in respect of processing of Personal Information for Services that takes place within that party's own systems. Cardinal's storage, processing, and transmission of any payment instrument data shall comply with the Payment Card Industry Data Security Standard (PCI-DSS), and Cardinal shall regularly validate its compliance. Upon Customer's request, Cardinal shall provide Customer with written confirmation of its PCI-DSS compliance status.

8 **Processors and Staff**. Cardinal shall ensure that any person or entity acting under its authority, including a data processor, shall be obligated in writing to treat the Customer Personal Information confidentially and to Process the Customer Personal Information only on instructions from Cardinal in accordance with applicable laws or regulations governing the same.

9 **Security Breach.** In the event of a Security Breach related to the Service, the party on whose systems the Security Breach occurred (the "Breaching Party") shall be responsible for handling the Security Breach and shall: (i) investigate the circumstances, extent and causes of the Security Breach; (ii) notify the non-Breaching party without undue delay upon becoming aware of an actual Security Breach affecting Customer Personal Information, and (iii) make any notifications required under Applicable Data Protection Law including as applicable: notifying a Supervisory Authority of the Security Breach and communicating the Security Breach to the relevant Data Subjects.

9.1 If either party is a Breaching Party, the other party shall cooperate and assist the Breach Party as necessary for the Breaching Party to communicate the Security Breach to the relevant Data Subjects.

9.2 Except as required by applicable law or regulation, the Breaching Party will not make (or permit any third party to make) any statement concerning the Security Breach that directly or indirectly references the no-Breaching Party, unless the other party provides its explicit written authorization.

9.3 To the extent that a Security Breach was caused by one party or its End Users, such party shall be responsible for the costs arising from the provision of assistance by the other party under this section 9.

10 **Miscellaneous**. The terms of this DPA shall apply only to the extent required by Applicable Data Protection Law. To the extent not inconsistent herewith, the applicable provisions of the Agreement(s) (including without limitation, indemnifications, limitations of liability, enforcement, and interpretation) shall apply to this DPA. In the event of any conflict between this DPA and the terms of an applicable Agreement, the terms of this DPA shall control solely with respect to data processing terms where required by Applicable Data Protection Law, and, in all other respects, the terms of the applicable Agreement shall control. Notwithstanding any term or condition of the DPA, this DPA does not apply to any data or information that does not relate to one or more identifiable individuals under Applicable Data Protection Law, such as data that has been aggregated, de-identified or anonymized, or to the extent that Cardinal and you have entered separate data processing terms that address the subject matter hereof.

Cardinal shall pay reasonable costs related to a Security Breach, but only to the extent (i) that Customer is a direct licensee of Cardinal (as opposed to a customer of a reseller of, or other third party offering Cardinal's products and services) and (ii) such Security Breach is caused by or attributable to Cardinal's negligence or breach of this DPA, including reasonable costs of breach notifications and any credit monitoring for Data Subjects required by Customer, up to an amount not to exceed one (1) million US dollars ($1,000,000.00), or such amount otherwise expressly mandated by Applicable Data Protection Law, solely to the extent such mandated amount exceeds one million US dollars.

11 **Definitions**. Unless otherwise defined in the Agreement (including this DPA), all terms in this DPA shall have the definitions given to them in Applicable Data Protection Law.

| | |
|---|---|
| "Applicable Data Protection Law" | means any law or regulation pertaining to data protection, privacy, and/or the Processing of Personal Information, to the extent applicable in respect of a party's obligations under the Agreement and this DPA. For illustrative purposes only, "Applicable Data Protection Laws" include, without limitation, and to the extent applicable, the General Data Protection Regulation (Regulation (EU) 2016/679 (the "GDPR"), UK Data Protection Laws, the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 and its implementing regulations (collectively, the "GLBA"), Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5 ("PIPEDA"), Swiss DP Laws and any associated regulations or any other legislation or regulations that |

| | |
|---|---|
| | transpose or supersede the above or are deemed substantially similar to the above. |
| "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 Applicable Data Protection Law. |
| "Personal Information" | means all data or information, in any form or format, that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer ("Data Subject") or household or that is regulated as "personal data," "nonpublic personal information" or "personal information," or otherwise under Applicable Data Protection Law. For the avoidance of doubt, this includes any information relating to a Data Subjects as defined in the Agreement. |
| "Process" or "Processed" or "Processing" | means any operation or set of operations which is performed upon Personal Information, whether or not by automatic means, such as access, collection, recording, organization, storage, adaptation or alteration, retrieval, disclosure or otherwise making available, duplication, transmission, combination, blocking, redaction, erasure or destruction. |
| "Security Breach" | means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Information. A Security Breach includes a "personal data breach" (as defined in the GDPR), a "breach of security of a system", a "breach of security safeguards" (as defined in PIPEDA) or similar term (as defined in any other applicable privacy laws) as well as any other event that compromises the security, confidentiality or integrity of Personal Information. |
| "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. |
| "Transfer" | means to transmit or otherwise make Customer Personal Information available across national borders in circumstances which are restricted by Applicable Data Protection law. |
| "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. |

| | |
|---|---|
| "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 |

**Schedule A: General Data Protection Regulation**

This GDPR Schedule applies in addition to any terms set forth in the body of the DPA (and is incorporated therein) when the GDPR applies to your use of Services or to the extent Applicable Data Protection Law imposes a comparable requirement outlined under this Schedule. Capitalized terms not defined herein have the meaning assigned to them under the DPA. To the extent there are any conflicts between this GDPR Schedule and the DPA, this GDPR Schedule shall prevail.

1 **Controller designation**. The parties acknowledge and agree that in respect of the Processing of such Customer Personal Information for the purpose of the Service, both Customer and Cardinal shall act as "joint controllers" (as defined in the GDPR). Cardinal qualifies as the Controller for operating, maintaining and updating the Service and Customer qualifies as the Controller for the transmission of Personal Information to the Service. The obligations in this DPA, including this Schedule A, shall constitute the written arrangement allocating responsibilities between joint controllers required under Article 26 GDPR with respect to the Services.

2 **Cross-Border Transfers**. Customer agrees and acknowledges that Cardinal Transfers and stores certain Customer Personal Information (including relating to individuals located in the European Economic Area ("EEA"), the UK or Switzerland) in the United States.

2.1 **Transfers subject to the GDPR, UK GDPR or Swiss DP Laws**: Module 1 (transfer controller to controller) of the EEA Standard Contractual Clauses shall apply with respect to any Transfer of Customer Personal Information from the EEA, UK or Switzerland to Cardinal in the United States, solely when Cardinal is acting as a controller for the purposes of the Service. The parties acknowledge and agree that Module 1 (transfer controller to controller) of the EEA Standard Contractual Clauses is hereby incorporated by reference and;

2.1.1 Customer and any of its commonly owned or controlled affiliates that have signed an Agreement for Services ("Customer Entities") shall be deemed to be "data exporters" and Cardinal and any and any of its affiliated entities in the United States or other third countries and territories ("Cardinal Entities") shall be the "data importer";

2.1.2 Clause 7 – *Docking clause* shall apply;

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

2.1.4 Clause 13(a) – *Supervision Where the data exporter 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."*

2.1.4.1. *Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of the GDPR the following shall apply: "The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority."*

2.1.4.2. *Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of the GDPR in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of the GDPR, the following shall apply: "The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose*

*behavior is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority."*

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

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

2.1.7 the information in Exhibit 2 (Table 1) of this GDPR Schedule is incorporated into Annexes 1, 2 and 3 of the EEA Standard Contractual Clauses.

2.1.8 **Transfers subject to the UK GDPR:** where the Transfer is subject to the UK GDPR, the EEA Standard Contractual Clauses shall be read in accordance with, and deemed amended by, the provisions of Part 2 (Mandatory Clauses) of the UK IDTA. For the purposes of Table 4 in Part 1 (Tables) of the UK IDTA, the parties select the "neither party" option. ~~, and~~Otherwise, the Parties confirm that the information required for the purposes of Part 1 (Tables) of the UK IDTA is set out in Exhibit 2**.**

2.1.9 if there is any conflict or inconsistency between a term in the body of this DPA, an Agreement and a term in Module 1 (transfer controller to controller) of the EEA Standard Contractual Clauses incorporated into this DPA, the term in the EEA Standard Contractual Clauses shall take precedence.

**EXHIBIT 1**
**Details of Processing Customer Personal Information**

**The table below includes additional details of the Processing of Customer Personal Information in respect of the Services.**

| Nature and purpose of processing | Types of Personal Information | Categories of data subjects related to the Personal Information |
|---|---|---|
| The Service is a 3-D Secure based consumer-authentication solution that uses a data-driven approach for transaction fraud prevention and enables real-time risk assessment of online 3-D Secure transactions. The Service provides users with a rules portal as a means for users to make their own risk decision. This includes the generation of a risk score through the Service's proprietary model. Customer Personal Information is used to support the creation and enhancement of the Service, including tools and models for use by Customer and any other customers of Cardinal.<br><br>To provide the Service, Cardinal transfers Customer Personal Information to acquiring banks, issuing banks, payment processors providing services on behalf of acquiring banks, credit/debit card companies, or service providers. | Cardinal will use required transaction information, including, without limitation, card number, cardholder name, billing address, shipping address email address, phone number, IP address, device characteristics, transaction amount, for Processing the authentication request with the Customer.<br><br>Further detail is included in the applicable Services Documentation provided at the time of implementation of the Service. | Data Subjects as defined under the Agreement, including: credit card holders, debit card users and all consumers whose cardholder or bank account data is submitted to the Service. |

**EXHIBIT 2**
**INFORMATION REQUIRED FOR THE EEA STANDARD CONTRACTUAL CLAUSES**

**Table 1: Information to be incorporated into the EEA Standard Contractual Clauses**

| **Information to be incorporated into the EEA Standard Contractual Clauses** | |
|---|---|
| **ANNEX I A. List of Parties** | |
| **Data EXPORTER identity and contact details** | |
| *Name* | Customer Entities |
| *Address* | To be provided on request |
| *Contact person's name, position and contact details:* | To be provided on request |
| *Activities relevant to the data transferred under these Clauses:* | As set out in the table in Exhibit 1 under "Nature and Purpose of the Processing". |
| *Role (controller/processor):* | Controller |
| **Data IMPORTER identity and contact details** | |
| *Name* | Cardinal Entities |
| *Address* | 900 Metro Center Boulevard<br>Foster City, CA 94404<br>U.S.A. |
| *Contact person's name, position and contact details:* | privacy@visa.com |
| *Activities relevant to the data transferred under these Clauses:* | As set out in the table in Exhibit 1 under "Nature and Purpose of the Processing". |
| *Role (controller/processor):* | Controller |
| **ANNEX I B. Description of Transfer** | |
| *Categories of data subjects whose personal data is transferred* | As set out in the table in Exhibit 1 under "Categories of Data Subjects". |
| *Categories of personal data transferred* | As set out in the table in Exhibit 1 under "Types of Personal Information". |

| | |
|---|---|
| *Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.* | Not Applicable |
| *The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).* | Continuous |
| *Nature of the processing* | As set out in the table in Exhibit 1 under "Nature and Purpose of the Processing". |
| *Purpose(s) of the data transfer and further processing* | As set out in the table in Exhibit 1 under "Nature and Purpose of the Processing". |
| *The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period* | Personal data will be retained in accordance with Cardinal's retention policies, for only as long as is required to meet Cardinal's legal, regulatory and operational requirements and as necessary to perform services. |
| *For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing* | As set out in the table in Exhibit 1 under "Nature and Purpose of the Processing". |
| **Annex I C. Competent Supervisory Authority** | |
| *Competent supervisory authority/ies* | To be provided by the data exporter on request. |
| **ANNEX II Technical and Organizational Measures Including Technical and Organizational Measures to Ensures Security of the Data** | |
| *Description of the technical and organizational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.* | CardinalCommerce is certified as compliant with all standards established by the Payment Card Industry Data Security Standards (together with any successor organization thereto, "PCI DSS") that are applicable to Cardinal Corporation and its affiliates (such standards, the "PCI Standards"). As evidence of compliance, Cardinal will provide its current Attestation of Compliance signed by a Payment Card Industry Qualified Security Assessor upon Customer's written request.<br><br>CardinalCommerce maintains and enforces commercially reasonable information security and |

| | |
|---|---|
| | physical security policies, procedures and standards, that are designed (i) to insure the security and confidentiality of Customer's records and information, (ii) to protect against any anticipated threats or hazards to the security or integrity of such records, and (iii) to protect against unauthorized access to or use of such records or information which could result in substantial harm (the "Visa Information Security Program"). At a minimum, the Visa Information Security Program is designed to meet the standards set forth in ISO 27002 published by the International Organization for Standardization, as well as any revisions, versions or other standards or objectives that supersede or replace the foregoing.<br><br>CardinalCommerce engages its independent certified public accountants to conduct a review of Cardinal Corporation's operations and procedures at Cardinal Corporation's cost. The accountants conduct the review in accordance with the American Institute of Certified Public Accounts Statement on Standards for Attestation Engagements No. 18 SOC I Type II ("SSAE 18") and record their findings and recommendations in a report to Cardinal Corporation. Upon request, and subject to standard confidentiality obligations, Cardinal will provide its most recent SSAE 18 and, in Cardinal's s reasonable discretion, additional information reasonably requested to address questions or concerns regarding the SSAE 18's findings. |
| *For transfers to (sub-) processors, also describe the specific technical and organizational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter* | Not applicable. |
| **ANNEX III LIST OF SUB-PROCESSORS**<br>*The controller has authorized the use of the following sub-processors:* | |
| Not applicable to Module 1. | |