Entrust Datacard
Trusted Identities | Secure Transactions

DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") supplements and forms part of the written or electronic agreement(s) (individually and collectively the "**Agreement**") between Entrust Datacard and its customer ("**Customer**") for the purchase, access to, and/or licensing of products, services and/or platforms (collectively the "**Services**") from the Entrust Datacard entity and the Customer entity identified in the Agreement, to reflect the parties' agreement with regard to the Processing of Personal Data.

By signing the Agreement, Customer agrees to the terms and conditions set out in this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws and Regulations, in the name of and on behalf of its Authorized Affiliates (as defined below), if and to the extent Entrust Datacard processes Personal Data for which such Authorized Affiliates qualify as the Controller. For the purposes of this DPA only, and except where indicated otherwise, the term "Customer" shall include Customer and Authorized Affiliates.

This DPA shall be effective for the term of the Agreement.

In the course of providing the Services to Customer pursuant to the Agreement, Entrust Datacard may Process Personal Data on behalf of Customer and the parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

DATA PROCESSING TERMS

1. DEFINITIONS

1.1. In this DPA, the following terms shall have the following meanings:

(a) "**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

(b) "**Authorized Affiliate**" means any of Customer's Affiliate(s) which (a) is subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (b) is permitted to use the Services pursuant to the Agreement between Customer and Entrust Datacard, but has not signed its own agreement with Entrust Datacard and is not a "Customer" as defined under the Agreement.

(c) "**Controller**" means the entity which determines the purposes and means of the Processing of Personal Data.

Entrust Datacard
Trusted Identities | Secure Transactions

(d) "**Data Protection Laws and Regulations**" means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland and the United Kingdom, applicable to the Processing of Personal Data under the Agreement.

(e) "**Data Subject**" means the identified or identifiable person to whom Personal Data relates.

(f) "**Entrust Datacard**" means the Entrust Datacard entity which is a party to the Agreement.

(g) "**Entrust Datacard Group**" means Entrust Datacard and its Affiliates engaged in the Processing of Personal Data.

(h) "**GDPR**" means the 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, and repealing Directive 95/46/EC (General Data Protection Regulation).

(i) **"Internal Data Handling Policy"** means the Entrust Datacard internal Personal Data handling policy applicable to its products, services and/or platforms, as updated from time to time, and accessible in summary form upon written request to Entrust Datacard.

(j) "**Personal Data**" means any information relating to (i) an identified or identifiable natural person and, (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws and Regulations).

(k) "**Processing**" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

(l) "**Processor**" means the entity which Processes Personal Data on behalf of the Controller.

(m) "**Standard Contractual Clauses**" means the terms and conditions agreed to by and between Customer and Entrust Datacard (by virtue of their entering into the Agreement) and attached hereto as Schedule 3 pursuant to the European Commission's decision (C(2010)593) of 5 February 2010 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

Entrust Datacard
Trusted Identities | Secure Transactions

(n) "**Sub-processor**" means any Processor engaged by Entrust Datacard or a member of the Entrust Datacard Group.

(o) "**Supervisory Authority**" means an independent public authority which is established by an EU Member State pursuant to the GDPR.

2. PROCESSING OF PERSONAL DATA

2.1. **Roles of the Parties**. The parties acknowledge and agree that with regard to the Processing of Personal Data, Customer is the Controller, Entrust Datacard is the Processor and that Entrust Datacard or members of the Entrust Datacard Group will engage Sub-processors pursuant to the requirements set forth in Section 5 "Sub-processors" below.

2.2. **Customer's Processing of Personal Data.** Customer shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations. For the avoidance of doubt, Customer's instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data.

2.3. **Entrust Datacard's Processing of Personal Data**. Entrust Datacard shall treat Personal Data as Confidential Information and shall only Process Personal Data on behalf of and in accordance with Customer's documented instructions for the following purposes: (i) Processing in accordance with the Agreement; (ii) Processing initiated by end users in their use of the Services; and (iii) Processing to comply with other documented reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement. Entrust Datacard shall immediately inform Customer if, in Entrust Datacard's opinion, an instruction infringes the Data Protection Laws and Regulations.

2.4. **Details of the Processing.** The subject-matter of Processing of Personal Data by Entrust Datacard is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule 2 (Details of the Processing) to this DPA.

3. RIGHTS OF DATA SUBJECTS

3.1. **Data Subject Requests.** Entrust Datacard shall, to the extent legally permitted, promptly notify Customer if Entrust Datacard receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, object to the Processing, or its right not to be subject to an automated individual decision making ("**Data Subject Request**"). Taking into account the nature of the Processing, Entrust Datacard shall assist Customer by appropriate technical

and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. In addition, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, Entrust Datacard shall upon Customer's request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent Entrust Datacard is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws and Regulations. To the extent legally permitted, Customer shall be responsible for any costs arising from Entrust Datacard's provision of such assistance.

4. ENTRUST DATACARD PERSONNEL

4.1. **Confidentiality**. Entrust Datacard shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements. Entrust Datacard shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

4.2. **Reliability**. Entrust Datacard shall take commercially reasonable steps to ensure the reliability of any Entrust Datacard personnel engaged in the Processing of Personal Data.

4.3. **Limitation of Access**. Entrust Datacard shall ensure that Entrust Datacard's access to Personal Data is limited to those personnel performing Services in accordance with the Agreement.

4.4. **Data Processor Point of Contact**. If Customer has any questions relating to data protection in relation to the Processing by Entrust Datacard, Customer may send such questions to *privacy@entrustdatacard.com*.

5. SUB-PROCESSORS

5.1. **Appointment of Sub-processors**. Customer acknowledges and agrees that (a) Entrust Datacard's Affiliates may be retained as Sub-processors; and (b) Entrust Datacard and Entrust Datacard's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services. Entrust Datacard or a Entrust Datacard Affiliate has entered into a written agreement with each Sub-processor containing data protection obligations not less protective than those in this Agreement with respect to the protection of Personal Data to the extent applicable to the nature of the Services provided by such Sub-processor. Customer acknowledges that Entrust Datacard Corporation is located in the United States and is involved in providing the Services to Customer either directly or through other members of the Entrust Datacard Group. In either case, Customer agrees to the Standard Contractual Clauses set out in Schedule 3 and acknowledges that Sub-processors may be appointed by Entrust Datacard in accordance with Clause 11 of Schedule 3.

Entrust Datacard
Trusted Identities | Secure Transactions

5.2. **List of Current Sub-processors and Notification of New Sub-processors**. Entrust Datacard shall make available to Customer the current list of Sub-processors for the Services. Such Sub-processor lists shall include the identities of those Sub-processors and their country of location ("**Sub-processor Lists**").

5.3. **Objection Right for New Sub-processors**. Customer may object to Entrust Datacard's use of a new Sub-processor by notifying Entrust Datacard promptly in writing within ten (10) business days after receipt of Entrust Datacard's communication advising of the new Sub-processor. In the event Customer objects to a new Sub-processor, as permitted in the preceding sentence, Entrust Datacard will use reasonable efforts to address Customer's objections. If Entrust Datacard is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Customer may terminate the applicable Agreement with respect only to those Services which cannot be provided by Entrust Datacard without the use of the objected-to new Sub-processor by providing written notice to Entrust Datacard. Entrust Datacard will refund Customer any prepaid fees covering the remainder of the term of such Agreement following the effective date of termination with respect to such terminated Services, without imposing a penalty for such termination on Customer.

5.4. **Liability.** Entrust Datacard shall be liable for the acts and omissions of its Sub-processors to the same extent Entrust Datacard would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

6. SECURITY

6.1. **Controls for the Protection of Personal Data**. Entrust Datacard shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Personal Data), confidentiality and integrity of Personal Data, as set forth in the Internal Data Handling Policy. Entrust Datacard regularly monitors compliance with these measures.

6.2. **Third-Party Certifications and Audits**. Entrust Datacard has obtained the third-party certifications and audits set forth in the Internal Data Handling Policy. Upon Customer's written request (at reasonable intervals), and subject to the confidentiality obligations set forth in the Agreement, Entrust Datacard shall make available to Customer that is not a competitor of Entrust Datacard (or Customer's independent, third-party auditor that is not a competitor of Entrust Datacard) information regarding Entrust Datacard Group's compliance with the obligations set forth in this DPA in the form of the third party certifications and audits set forth in the Internal Data Handling Policy. Customer may contact Entrust Datacard in accordance with the "Notices" Section of the Agreement to request an on-site audit of Entrust Datacard's procedures relevant to the protection of Personal Data, but only to the extent required under applicable Data Protection Laws and Regulations. Customer shall reimburse Entrust Datacard for any time expended for any such

on-site audit at Entrust Datacard's then-current rates, which shall be made available to Customer upon request. Before the commencement of any such on-site audit, Customer and Entrust Datacard shall mutually agree upon the scope, timing, and duration of the audit, in addition to the reimbursement rate for which Customer shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by Entrust Datacard. Customer shall promptly notify Entrust Datacard with information regarding any non-compliance discovered during the course of an audit, and Entrust Datacard shall use commercially reasonable efforts to address any confirmed non-compliance.

7. PERSONAL DATA INCIDENT MANAGEMENT AND NOTIFICATION

7.1. Entrust Datacard maintains security incident management policies and procedures specified in the Internal Data Handling Policy and shall, notify Customer without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data, transmitted, stored or otherwise Processed by Entrust Datacard or its Sub-processors of which Entrust Datacard becomes aware (a "**Personal Data Incident**"). Entrust Datacard shall make reasonable efforts to identify the cause of such Personal Data Incident and take those steps as Entrust Datacard deems necessary and reasonable in order to remediate the cause of such a Personal Data Incident to the extent the remediation is within Entrust Datacard's reasonable control. The obligations herein shall not apply to incidents that are caused by Customer or end users.

8. RETURN AND DELETION OF PERSONAL DATA

8.1. Entrust Datacard shall return Personal Data to Customer and, to the extent allowed by applicable law, delete Personal Data in accordance with the procedures and timeframes specified in the Internal Data Handling Policy.

9. AUTHORIZED AFFILIATES

9.1. **Contractual Relationship**. The parties acknowledge and agree that, by executing the Agreement, the Customer agrees to the terms and conditions of this DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, thereby establishing a separate DPA between Entrust Datacard and each such Authorized Affiliate is subject to the provisions of the Agreement and this Section 9 and Section 10. Each Authorized Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the avoidance of doubt, an Authorized Affiliate is not and does not become a party to the Agreement, and is only a party to the DPA. All access to and use of the Services and related content by Authorized Affiliates must comply with the terms and conditions of the Agreement and any violation of the terms and conditions of the Agreement by an Authorized Affiliate shall be deemed a violation by Customer.

Entrust Datacard
Trusted Identities | Secure Transactions

9.2. **Communication**. The Customer that is the contracting party to the Agreement shall remain responsible for coordinating all communication with Entrust Datacard under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates.

9.3. **Rights of Authorized Affiliates**. Where an Authorized Affiliate becomes a party to the DPA with Entrust Datacard, it shall to the extent required under applicable Data Protection Laws and Regulations be entitled to exercise the rights and seek remedies under this DPA, subject to the following:

9.3.1. Except where applicable Data Protection Laws and Regulations require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against Entrust Datacard directly by itself, the parties agree that (i) solely the Customer that is the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Authorized Affiliate, and (ii) the Customer that is the contracting party to the Agreement shall exercise any such rights under this DPA not separately for each Authorized Affiliate individually but in a combined manner for all of its Authorized Affiliates together (as set forth, for example, in Section 9.3.2, below).

9.3.2. The parties agree that the Customer that is the contracting party to the Agreement shall, when carrying out an on-site audit of the procedures relevant to the protection of Personal Data, take all reasonable measures to limit any impact on Entrust Datacard and its Sub-Processors by combining, to the extent reasonable possible, several audit requests carried out on behalf of different Authorized Affiliates in one single audit.

10. LIMITATION OF LIABILITY

10.1. Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorized Affiliates and Entrust Datacard, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together. For the avoidance of doubt, Entrust Datacard's and its Affiliates' total liability for all claims from the Customer and all of its Authorized Affiliates arising out of or related to the Agreement and each DPA shall apply in the aggregate for all claims under both the Agreement and all DPAs established under this Agreement, including by Customer and all Authorized Affiliates, and, in particular, shall not be understood to apply individually and severally to Customer and/or to any Authorized Affiliate that is a contractual party to any such DPA. Also for the avoidance of doubt, each reference to the DPA in this DPA means this DPA including its Schedules and Appendices.

11. EUROPEAN SPECIFIC PROVISIONS

11.1. **GDPR**. Entrust Datacard will Process Personal Data in accordance with the GDPR requirements directly applicable to Entrust Datacard's provision of its Services.

Entrust Datacard
Trusted Identities | Secure Transactions

11.2. **Data Protection Impact Assessment**. Upon Customer's request, Entrust Datacard shall provide Customer with reasonable cooperation and assistance needed to fulfil Customer's obligation under the GDPR to carry out a data protection impact assessment related to Customer's use of the Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Entrust Datacard. Entrust Datacard shall provide reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to Section 11.2 of this DPA, to the extent required under the GDPR.

11.3. **Transfer mechanisms for data transfers**. Subject to the additional terms in Schedule 1, the Standard Contractual Clauses set forth in Schedule 3 to this DPA apply to the Services to the extent such transfers are subject to such Data Protection Laws and Regulations.

12. PARTIES TO THIS DPA

12.1. The Agreement specifies which Entrust Datacard entity is party to this DPA. In addition, Entrust Datacard Corporation is a party to the Standard Contractual Clauses in Schedule 3. Where Entrust Datacard is a different legal entity than Entrust Datacard Corporation, Entrust Datacard is carrying out the obligations of the data importer as set out in Schedule 3 "Standard Contractual Clauses" on behalf of Entrust Datacard Corporation.

13. LEGAL EFFECT

13.1. This DPA shall only become legally binding between Customer and Entrust Datacard (and Entrust Datacard Corporation, if different) when the Agreement is signed by both parties.

List of Schedules

Schedule 1: Transfer Mechanisms for European Data Transfers

Schedule 2: Details of the Processing

Schedule 3: Standard Contractual Clauses

Entrust Datacard
Trusted Identities | Secure Transactions

SCHEDULE 1 - TRANSFER MECHANISMS FOR EUROPEAN DATA TRANSFERS

1. STANDARD CONTRACTUAL CLAUSES

1.1. **Standard Contractual Clauses**. The Standard Contractual Clauses and the additional terms specified in this Section 1 apply to (i) the Customer legal entity that has executed the Agreement as a data exporter and its Authorized Affiliates and, (ii) all Affiliates of Customer established within the European Economic Area, Switzerland and the United Kingdom, which have signed an Agreement for the Services. For the purpose of the Standard Contractual Clauses and this Section 1, the aforementioned entities shall be deemed "data exporters".

1.2. **Instructions**. This DPA and the Agreement are Customer's complete and final documented instructions at the time of signature of the Agreement to Entrust Datacard for the Processing of Personal Data. Any additional or alternate instructions must be agreed upon separately. For the purposes of Clause 5(a) of the Standard Contractual Clauses, the following is deemed an instruction by the Customer to process Personal Data: (a) Processing in accordance with the Agreement; (b) Processing initiated by end users in their use of the Services and (c) Processing to comply with other reasonable documented instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement.

1.3. **Appointment of new Sub-processors and List of current Sub-processors**. Pursuant to Clause 5(h) of the Standard Contractual Clauses, Customer acknowledges and expressly agrees that (a) Entrust Datacard's Affiliates may be retained as Sub-processors; and (b) Entrust Datacard and Entrust Datacard's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services. Entrust Datacard shall make available to Customer the current list of Sub-processors in accordance with Section 5.2 of this DPA.

1.4. **Notification of New Sub-processors and Objection Right for new Sub-processors**. Pursuant to Clause 5(h) of the Standard Contractual Clauses, Customer acknowledges and expressly agrees that Entrust Datacard may engage new Sub-processors as described in Sections 5.2 and 5.3 of the DPA.

1.5. **Copies of Sub-processor Agreements**. The parties agree that the copies of the Sub-processor agreements that must be provided by Entrust Datacard to Customer pursuant to Clause 5(j) of the Standard Contractual Clauses may have all commercial information, or clauses unrelated to the Standard Contractual Clauses or their equivalent, removed by Entrust Datacard beforehand; and, that such copies will be provided by Entrust Datacard, in a manner to be determined in its discretion, only upon request by Customer.

1.6. **Audits and Certifications**. The parties agree that the audits described in Clause 5(f) and Clause 12(2) of the Standard Contractual Clauses shall be carried out in accordance with the

following specifications:

Upon Customer's request, and subject to the confidentiality obligations set forth in the Agreement, Entrust Datacard shall make available to Customer that is not a competitor of Entrust Datacard (or Customer's independent, third-party auditor that is not a competitor of Entrust Datacard) information regarding the Entrust Datacard Group's compliance with the obligations set forth in this DPA in the form of the third-party certifications and audits set forth in the Internal Data Handling Policy to the extent Entrust Datacard makes them generally available to its customers. Customer may contact Entrust Datacard in accordance with the "Notices" Section of the Agreement to request an on-site audit of the procedures relevant to the protection of Personal Data. Customer shall reimburse Entrust Datacard for any time expended for any such on-site audit at Entrust Datacard's then-current professional services rates, which shall be made available to Customer upon request. Before the commencement of any such on-site audit, Customer and Entrust Datacard shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which Customer shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by Entrust Datacard. Customer shall promptly notify Entrust Datacard with information regarding any non-compliance discovered during the course of an audit.

1.7. **Certification of Deletion**. The parties agree that the certification of deletion of Personal Data that is described in Clause 12(1) of the Standard Contractual Clauses shall be provided by Entrust Datacard to Customer only upon Customer's request.

1.8. **Conflict**. In the event of any conflict or inconsistency between the body of this DPA and any of its Schedules (not including the Standard Contractual Clauses) and the Standard Contractual Clauses in Schedule 3, the Standard Contractual Clauses shall prevail.

Entrust Datacard
Trusted Identities | Secure Transactions

SCHEDULE 2 - DETAILS OF THE PROCESSING

Nature and Purpose of Processing

Entrust Datacard will Process Personal Data as necessary to perform the Services pursuant to the Agreement, as further specified in the Services-related documentation, and as further instructed by Customer in its use of the Services.

Duration of Processing

Subject to Section 8 of the DPA, Entrust Datacard will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

Categories of Data Subjects

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Prospects, customers, business partners and vendors of Customer (who are natural persons)
- Employees or contact persons of Customer's prospects, customers, business partners and vendors
- Employees, agents, advisors, freelancers of Customer (who are natural persons)
- Customer's end users authorized by Customer to use the Services

Type of Personal Data

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- First and last name
- Title
- Position
- Employer
- Contact information (company, email, phone, physical business address)
- ID data
- Professional life data

Entrust Datacard
Trusted Identities | Secure Transactions

- Personal life data
- Connection data
- Localisation data

Entrust Datacard
Trusted Identities | Secure Transactions

SCHEDULE 3 - STANDARD CONTRACTUAL CLAUSES

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

Name of the data exporting organisation: Customer as detailed in the Agreement.

Address and other contact information: See Customer address and contact details as set out in the Agreement

And

Name of the data importing organisation: Entrust Datacard Corporation

Address: 1187 Park Place, Shakopee, Minnesota 55379-3817 USA

Tel.: 1-952-988-2715 ; fax: 1-952-932-9409 ; e-mail: privacy@entrustdatacard.com

Other information needed to identify the organisation: Not applicable

(the data importer)

each a “party”; together “the parties”,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Entrust Datacard
Trusted Identities | Secure Transactions

Clause 1

Definitions

For the purposes of the Clauses:

(a) '*personal data*', '*special categories of data*', '*process/processing*', '*controller*', '*processor*', '*data subject*' and '*supervisory authority*' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) *'the data exporter*' means the controller who transfers the personal data;

(c) *'the data importer*' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor*' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law*' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) '*technical and organisational security measures*' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Entrust Datacard
Trusted Identities | Secure Transactions

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

Entrust Datacard
Trusted Identities | Secure Transactions

1. The data importer agrees that if the data subject invokes against it third-party beneficiary and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

Entrust Datacard
Trusted Identities | Secure Transactions

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall

destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

Agreed by Customer by virtue of their signature of the Agreement.

On behalf of the data importer:

Name (written out in full): Lisa Tibbits

Position: Officer

Address: 1187 Park Place, Shakopee, Minnesota 55379-3817 USA

Agreed by Entrust Datacard by virtue of their signature of the Agreement.

Entrust Datacard
Trusted Identities | Secure Transactions

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and has been agreed by the parties by virtue of their signing the Agreement.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

Data Exporter is (i) the legal entity that has executed the Agreement and as a result has accepted the Standard Contractual Clauses as a Data Exporter and, (ii) all Affiliates (as defined in the Agreement) of Customer established within the European Economic Area (EEA) and Switzerland that have purchased Services on the basis of one or more Agreement(s).

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

Entrust Datacard is a provider of enterprise cloud authentication and fraud prevention computing solutions which processes personal data upon the instruction of the data exporter in accordance with the terms of the Agreement.

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

Data exporter may submit Personal Data to the Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Prospects, customers, business partners and vendors of data exporter (who are natural persons)
- Employees or contact persons of data exporter's prospects, customers, business partners and vendors
- Employees, agents, advisors, freelancers of data exporter (who are natural persons)
- Data exporter's end users authorized by data exporter to use the Services

Categories of data

The personal data transferred concern the following categories of data (please specify):

Entrust Datacard
Trusted Identities | Secure Transactions

Data exporter may submit Personal Data to the Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- First and last name
- Title
- Position
- Employer
- Contact information (company, email, phone, physical business address)
- ID data
- Professional life data
- Personal life data
- Connection data
- Localisation data

Processing operations

The Personal Data transferred will be subject to the following basic processing activities (please specify):

The objective of Processing of Personal Data by data importer is the performance of the Services pursuant to the Agreement.

Entrust Datacard
Trusted Identities | Secure Transactions

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and has been agreed by the parties by virtue of their signing the Agreement.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Reliability of Personnel: Entrust Datacard conducts background checks on all employees before employment, and employees and contractors receive information security training during onboarding as well as on an ongoing basis. All employees are required to read and sign Entrust Datacard's information security policies.

Compliance, audits, and certifications: Entrust Datacard, with the full commitment of its senior leadership, strongly believes that the fundamental principle to its success in innovation is its information security strategy. This strategy is based on adherence to enterprise-wide world-class governance, a set of controls and strict compliance with federal, financial, international, and industry regulations and policies such as:

- ISO 27001
- NIST 800-53
- Certificate Authority Browser (CAB) Forum Webtrust (may not apply for some products)

To ensure that the information security strategy is effective, Entrust Datacard enforces information security policies and procedures across its entire organization, as well as all business and technical projects. Governance, Risk and Compliance (GRC), Threat and Vulnerability Management (TVM), Security Architecture, Security Operations Center, Disaster Recovery, Business Continuity and Incident Response are the integral components of this strategy.

Incident Response:

At an operational level, Entrust Datacard has instituted a Security Incident Response Plan to oversee data security events identified or detected by the various technologies used to monitor and alert based on specific thresholds or circumstances. The objectives of the Security Incident Response Plan are to manage and coordinate data security incidents throughout all aspects of the Entrust Datacard computing environment regardless of location, product or process, as well as provide opportunities for educating our colleagues on risks and security controls in place.

Security Operation Center (SOC):

Entrust Datacard is committed to protecting the interest of stakeholders by maintaining a robust Security Operation Center (SOC). The SOC is a centralized unit that monitors the confidentiality, integrity, and availability of information technology infrastructure and deals with security on an organizational level.

Threat and Vulnerability Management (TVM):

Entrust Datacard has a continuous vulnerability discovery and remediation program. This process is built on industry certified tools and procedures and is facilitated by competent and experienced professionals. The Threat and Vulnerability Management (TVM) controls and measures are audited several times a year by qualified auditors to ensure we are compliant with applicable laws and industry standard frameworks.

Disaster Recovery:

Entrust Datacard is committed to protecting the interest of stakeholders in the event of an emergency or business disruption. Entrust Datacard therefore maintains a comprehensive organization-wide business continuity program to protect staff, safeguard corporate assets and environments, and to ensure continuous availability of its products and services. To support the Business Continuity Program, Entrust Datacard also maintains a Crisis Communications and Incident Response Plan to help strengthen our emergency response capability.

Business Continuity:

Entrust Datacard is committed to protecting the interest of stakeholders in the event of an emergency or business disruption. Entrust Datacard therefore maintains a comprehensive organization-wide Business Continuity Program that is consistent with the guidance issued by the (U.S.) National Fire Protection Association (NFPA) 1600 – Standard on Disaster/Emergency Management and Business Continuity Programs, and (International) ISO 22301 – Societal security – Business continuity management systems standards. The Business Continuity Plan identifies the functional roles and responsibilities of internal and external agencies, organizations and departments.

Product Security Pipeline Standard:

This document is a component of Entrust Datacard's information security program that includes Secure Software Delivery Lifecycle (SDLC) and vulnerability management as well as minimum baseline development (where applicable) for software and firmware products enterprise-wide. Vulnerability identification and remediation are a central focus with the goal to minimize the number of security flaws in Entrust Datacard products and services, and to minimize the impact to customers when such flaws are discovered. The processes described herein apply to Entrust Datacard products and services and components of a customer system that may be used in conjunction with an Entrust Datacard product or service. The program will ensure that SDLC processes are consistent with Entrust Datacard information security goals and expectations. Additionally, system baselines will be established to support Entrust Datacard software and firmware within the lifecycle (e.g., source repositories) and to support deployment into production environments. Where practical, system baselines will be aligned with compliance requirements.

Network Security:

Entrust Datacard maintains access controls and policies to manage what access is allowed to the Entrust Datacard network and systems from each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls. Entrust Datacard will maintain corrective action and incident response plans to respond to potential security threats.

Physical and Environment Security:

Entrust Datacard facilities hosting technology information assets are equipped with appropriate controls to restrict physical access to the facility. Physical entry controls include a means to identify personnel and visitors, and ensure the individual is authorized to access the secured area prior to entry. All entry to secured areas are logged and logs reviewed periodically. Personnel are informed of, and subject to, the guidelines established for working within secured areas. Access points such as delivery or loading areas, and other points where unauthorized persons may enter the facility, are controlled to restrict further entry, and, to the extent it is practical, isolated from information processing areas. Physical security measures include the capability to monitor company facilities to detect unauthorized or unlawful use. Entrust Datacard has a physical security plan that incorporates a defined procedure to report suspicious activity, identified security weaknesses, or potential security events, as well as an escalation procedure to communicate events to local law enforcement as appropriate. Facility staff and visitors are informed regarding these physical security procedures and their responsibility to report security events.

Information Transfer Policy:

Information to be transferred shall at all times be properly secured, in accord with its classification, regardless of the media employed to carry the information or the transmission mechanism. All information to be transferred shall be subject to inspection for malicious software code and other potential hazards to confidentiality, integrity or availability. When the use of encryption is required for safekeeping, such use shall be subject to all applicable security requirements as well as legal or regulatory controls. Information to be transferred shall be subject to established retention and disposal requirements. Information transfer facilities shall comply with all applicable laws and regulations. Information and software shall not be transferred with external parties until all relevant contractual and security requirements are satisfied, including formal written agreements where required.