ENTRUST ACTING AS CONTROLLER – GLOBAL

DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") forms part of the written or electronic agreement(s) (individually and collectively the "**Agreement**") between Entrust (as defined below) and its supplier ("**Vendor**") for the purchase, access to, and/or licensing of products, related services and/or platforms (collectively the "**Services**") by the Entrust entity identified in the Agreement to reflect the parties' agreement with regard to Vendor's Processing of Personal Data on behalf of Entrust. The terms used in this DPA shall have the meanings set forth in this DPA. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement. Except as modified in the DPA, the terms of the Agreement shall remain in full force and effect.

1. INSTRUCTIONS

1.1. This DPA has been pre-signed on behalf of Entrust Corporation, acting for itself and for and on behalf of its Affiliates. Unless otherwise incorporated by reference in an Agreement between the parties, to enter into this DPA, the Vendor must:

1.1.1. Have a written or electronic agreement with Entrust;

1.1.2. Provide contact information for a Data Processor Point of Contact;

1.1.3. Provide a list of sub-processors (if applicable);

1.1.4. Provide detailed technical and organizational measures;

1.1.5. Complete the signature block below by providing the name of the signatory, their signature, their position, the address of the Vendor, and the date the DPA was executed; and

1.1.6. Submit the completed and signed DPA to Entrust at privacy@entrust.com.

2. EFFECTIVENESS

2.1. This DPA will only be effective (as of the Effective Date) if executed and submitted to Entrust accurately and in full accordance with paragraph 1 above and this paragraph 2. If Vendor makes any deletions or other revisions to this DPA which are not explicitly agreed to by Entrust, this DPA will be deemed null and void.

2.2. This DPA shall be effective for the duration of the Agreement (or longer to the extent required by applicable law).

2.3. The parties agree that this DPA shall replace any existing DPA or other contractual provisions pertaining to the subject matter contained herein that the parties may have previously entered into in connection with the Services, and will be effective as of the

date Entrust receives a complete and executed DPA from the Vendor indicated in the signature block below (the "**Effective Date**").

3. DEFINITIONS

"Biometric Data" shall mean, collectively, "biometric identifiers," "biometric information," and equivalent terms, as such terms are defined in the Biometric Data Protection Laws and that Vendor is processing on behalf of Entrust in the course of providing the Services under the Agreement.

"Biometric Data Protection Laws" refers to all Data Protection Laws applicable to the Processing of Biometric Data, including without limitation the Illinois Biometric Information Privacy Act, 740 ILCS § 14/1, et seq.; Tex. Bus. & Com. Code §503.001, et seq.; and Wash. Rev. Code Ann. §19.375.020 et seq. (in each case, as may be amended, superseded, or replaced).

"**Controller**" is synonymous with "personally identifiable information controller" as such terms are defined in the Data Protection Laws and in ISO 27701 and refers to the entity that determines the purpose and means of Processing Personal Data.

"**Customer**" means an existing potential customer of Entrust.

"**Data Protection Laws**" refers to all applicable data protection and data privacy laws and regulations, including, but not limited to, the EU General Data Protection Regulation (GDPR), UK General Data Protection Regulation (UK GDPR), Switzerland's Federal Act on Data Protection (as implemented on 1 September 2023) (FADP), Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), Japan's Act on Protection of Personal Information (APPI), China's Personal Information Protection Law (PIPL), the California Consumer Privacy Act, the Colorado Privacy Act (CPA), the Virginia Consumer Data Protection Act (VCDPA), the Utah Consumer Privacy Act (UCPA), and the Connecticut Data Privacy Act (CTDPA) (in each case, as may be amended, superseded, or replaced).

"**Data Subject**" is synonymous with "personally identifiable information principal" as such terms are defined in the Data Protection Laws and in ISO 27701 and refers to the identified or identifiable person or household to whom Personal Data relates.

"**Entrust**" means the Entrust Corporation entity that is a party to the Agreement.

"**Personal Data**" shall have the meaning ascribed to "personally identifiable information," "personal information," "personal data" or equivalent terms as such terms are defined in the Data Protection Laws and in ISO 27701 that Vendor is processing on behalf of Entrust in the course of providing the Services under the Agreement. Personal Data includes Biometric Data.

"**Personal Data Incident**" shall have the meaning assigned in the Data Protection Laws to the term "personal data breach" or an analogous term and refers to any situation in which Vendor becomes aware that Entrust's Personal Data has been or is likely to have been accessed, disclosed, altered, lost, destroyed or used by unauthorized persons, in an unauthorized or unlawful manner.

"**Processing**" means any operation or set of operations that is performed on 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.

"**Processor**" is synonymous with "personally identifiable information processor" as defined in ISO 27701 and refers to the entity that Processes Personal Data on behalf of the Controller.

"**Standard Contractual Clauses (SCCs)**" means, in respect of Personal Data processed by Vendor on behalf of the Entrust in:

(a) the EEA and/or processing EEA Personal Data, the unchanged, EU Commission-approved version of the standard contractual clauses in Commission Decision 2021/914/EU ("the EU SCCs");

(b) the UK and/or processing UK Personal Data, the EU Commission-approved version of the standard contractual clauses in Commission Decision 2021/914/EU as amended by the UK GDPR Addendum to Entrust's Vendor DPA ("UK Vendor Addendum") as located at https://www.entrust.com/sites/default/files/documentation/licensingandagreements/uk-gdpr-addendum-to-entrusts-vendor-and-partner-dpa.pdf.

(c) Switzerland and/or processing Swiss Personal Data, a version of the clauses referenced in (a) above that is deemed to be modified as follows:

1) In these Clauses, the term EU Member State or Member State also includes Switzerland and the other EFTA States

2) The transfer of personal data shall, to the extent legally permitted, be governed by the provisions of the General Data Protection Regulation. The provisions of the FADP (are additionally applicable on a subsidiary basis, in which case references to provisions of the General Data Protection Regulation shall be understood to be referring to the equivalent provisions of the FADP as in force from time to time, mutatis mutandis.

3) The Federal Data Protection and Information Commissioner is the competent supervisory authority with regard to the transfer of personal data out of Switzerland.

To the extent the processing of personal data is governed by the FADP, the term 'personal data' also includes the data of legal entities.

(d) China and/or processing Chinese Personal Data, the Measures on the Standard Contract for the Cross-border Transfer of Personal Information and the accompanying Personal Information Export Standard Contract.

"**Sub-processor**" means any entity appointed by the Processor to Process Personal Data on behalf of the Controller.

4. DATA PROTECTION OBLIGATIONS

4.1. **Roles of the Parties.** Subject to the paragraph below in this section 4.1, the parties acknowledge and agree that regarding the Processing of Personal Data under the Agreement, Entrust is the Controller and Vendor is the Processor. Where Vendor receives Customer information from Entrust, Vendor will serve as a Sub-processor and will process Customer Personal Data in accordance with the terms of this DPA as if it were a Processor.

4.2. **Vendor's Processing of Personal Data.** Vendor shall treat Personal Data as

confidential and shall only Process Personal Data on behalf of and in accordance with Entrust's instructions and for the following purposes: (i) Processing for the specific purpose of performing the Services specified in the Agreement or as otherwise required by law; and (ii) Processing to comply with other documented reasonable instructions provided by Entrust where such instructions are consistent with the terms of the Agreement.

Vendor shall immediately inform Entrust if, in Vendor's opinion, an instruction is in violation of the Data Protection Laws. Additionally, Vendor shall inform Entrust if Vendor determines that it can no longer meet its obligations under the Data Protection Laws. For the avoidance of doubt, Vendor will not: (i) collect, retain, use, sell, or otherwise disclose Personal Data for any purpose other than for the specific purpose of performing the Services or as otherwise required by law; or (ii) combine Personal Data received from or on behalf of the Entrust, with Personal Data Vendor receives from or on behalf of another person or persons, or collects from its own interaction with the Data Subject, unless doing so is permitted by the Data Protection Laws.

4.3. **Details of the Processing.** The subject matter of Processing Personal Data by Vendor 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 Processed and the categories of Data Subjects for whom Personal Data is Processed are set forth in Schedule 1.

4.4. **Authorized Personnel.** Vendor shall grant access to the Personal Data undergoing Processing to authorized personnel only to the extent strictly necessary for implementing, managing and monitoring of the Agreement. Vendor shall also ensure only authorized personnel who have undergone appropriate training in the protection and handling of Personal Data and are bound in writing to respect the confidentiality of Personal Data, have access to Personal Data.

4.5. **Security Controls.** Vendor shall implement appropriate technical and organizational measures to maintain the security, confidentiality and integrity of Personal Data, including measures designed to protect against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Personal Data. Vendor shall adhere, at a minimum, to the technical and organizational measures set forth in Entrust's Vendor Information Security Addendum located at https://www.entrust.com/sites/default/files/documentation/licensingandagreements/entrust-security-addendum_v1-0.pdf.

4.6. **Sensitive Data.** If the Processing involves Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or Biometric Data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), Vendor shall apply specific restrictions and/or additional safeguards.

4.7. **Biometric Data.** Without limiting any other obligation set forth in this DPA, if the Processing involves Biometric Data, Vendor shall (i) comply with all Biometric Data Protection Laws, and reasonably assist with Entrust's compliance with all Biometric

Data Protection Laws; (ii) Process Biometric Data only for the specific purposes for which the Biometric Data was initially collected; (iii) upon Entrust's written request, permanently destroy Biometric Data in Vendor's control or possession; and (iv) immediately notify Entrust in the event Vendor has violated, or is at risk of violating, the Biometric Data Protection Laws.

4.8. **Government Requests.** Vendor shall provide commercially reasonable cooperation to assist Entrust in its response to any legally enforceable requests from data protection authorities or other law enforcement authorities relating to the Processing of Personal Data under the Agreement and this DPA. In the event that any such request is made directly to Vendor, Vendor shall not respond to such communication directly without Entrust's prior authorization, unless legally compelled to do so. If Vendor is required to respond to such a request, Vendor shall promptly notify Entrust and provide it with a copy of the request unless legally prohibited from doing so. Vendor shall also provide the minimum necessary to comply with the request.

4.9. **Data Subject Requests.** Vendor shall promptly notify Entrust of any requests from Data Subjects seeking to exercise their rights under the Data Protection Laws and, taking into account the nature of the Processing, assist Entrust by implementing appropriate technical and organizational measures, insofar as this is possible, to assist with Entrust's obligation to respond to such requests. To the extent that Personal Data is not accessible to Entrust in its use of the Services, Vendor shall, where legally permitted and upon Entrust's request, provide commercially reasonable efforts to assist Entrust in responding to such requests if responses to such requests are required by the Data Protection Laws. Vendor shall not respond the request itself, unless authorized to do so by Entrust.

4.10. **Data Protection Impact Assessment.** Vendor shall, upon Entrust's written request and taking into account the nature of Processing and information available, provide reasonable assistance to Entrust in connection with its obligations to perform a data protection impact assessment under Article 35 of the GDPR or equivalent provisions under the Data Protection Laws.

4.11. **Transfer Risk Assessments.** Vendor has no reason to believe that the third country laws in the destination applicable to the processing by Vendor, including any requirements to disclose Personal Data or measures authorizing access by public authorities, prevent Vendor from complying with this DPA. Vendor will make best efforts to provide Entrust with relevant information and cooperate with Entrust in performing any Transfer Risk Assessment required to ensure compliance with this DPA, including the EU Standard Contractual Clauses attached to this DPA.

4.12. **Return or Deletion of Personal Data.** Following termination of the Agreement, Vendor shall, at the choice of Entrust, delete all Personal Data Processed on behalf of Entrust and certify to Entrust that it has done so, or, return all Personal Data to Entrust and delete existing copies unless applicable law requires storage of the Personal Data. Until the Personal Data is deleted or returned, Vendor shall continue to ensure compliance with this DPA.

4.13. **Data Processor Point of Contact.** If Entrust has any questions regarding Processing of Personal Data by Vendor, Entrust may send such questions to the following email:

Vendor email address: _____

5. SUB-PROCESSORS

5.1. **Appointment of Sub-processors.** Entrust acknowledges and agrees that Vendor may engage Sub-processors in connection with provision of the Services. The current list of Sub-processors for the Services is available at the URL provided by the Vendor in Schedule 2. Vendor has Entrust's general authorization for the engagement of sub-processors from this list. The Sub-processor list includes the identities of all Sub-processors, their country of location, and the nature and duration of the Processing.

5.2. **Sub-processor Agreements.** Vendor shall enter into a written agreement with any engaged Sub-processor that contains data protection obligations no less protective than those contained in this DPA. At Entrust's request, Vendor shall provide a copy of such Sub-processor agreement and any subsequent amendments to Entrust. To the extent necessary to protect business secrets or other confidential information, including Personal Data, Vendor may redact the text of the agreement prior to sharing the copy. Vendor will notify Entrust of any failure by the Sub-processor to fulfil its contractual obligations. Vendor shall also agree to a third party beneficiary clause with the Sub-processor whereby, in the event Vendor has factually disappeared, ceased to exist in law or has become insolvent, Entrust shall have the right to terminate the Sub-processor contract and to instruct the Sub-processor to erase or return the Personal Data for which Entrust is the Data Controller.

5.3. **Notification of New Sub-processors.** Vendor will notify Entrust in writing of any changes to this list of Sub-processors at least thirty (30) days in advance.

5.4. **Objection to New Sub-processors.** Entrust may object to Vendor's use of a new Sub-processor by notifying Vendor in writing within ten (10) business days after receipt of Vendor's communication advising of the new Sub-processor. In the event Entrust reasonably objects to the use of a new Sub-processor, Vendor will use reasonable efforts to address Entrust's objections. If Vendor is unable to make available such change within a reasonable period, which shall not exceed ninety (90) days, Entrust may, in its full discretion, terminate the applicable Agreement in full or with respect only to those Services which cannot be provided by Vendor without the use of the objected-to new Sub-processor by providing written notice to Vendor. Vendor will refund Entrust 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 Entrust.

5.5. **Liability.** Vendor shall be liable for the acts and omissions of its Sub-processors to the same extent Vendor would be liable if performing the services of each Sub-processor directly under the terms of this DPA.

5.6. **Third-Party Beneficiary.** Vendor shall agree to a third-party beneficiary clause with

the sub-processor whereby, in the event Vendor has factually disappeared, ceased to exist in law or become insolvent, Entrust shall have the right to instruct the Sub-processor to erase the Personal Data.

6. PERSONAL DATA INCIDENTS

6.1. Vendor shall notify Entrust without undue delay (and in any event within forty-eight (48) hours) after becoming aware of a Personal Data Incident. Vendor shall identify: (i) the cause of the Personal Data Incident, (ii) the nature of the Personal Data including where possible, the categories and approximate number of Data Subject concerned and the categories and approximate number of Personal Data records concerned, (iii) the likely consequences of the Personal Data Incident, (iv) the measures taken or proposed to be taken by Vendor to address the Personal Data Incident, including, where appropriate, measures to mitigate its possible adverse effects and (v) the details of a contact point where more information concerning the Personal Data Incident can be obtained. Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

6.2. **Notifications.** Vendor shall cooperate and assist Entrust with any obligations to notify data protection authorities or affected data subjects under Data Protection Laws considering the nature of the Processing and the information available to Vendor.

7. INTERNATIONAL DATA TRANSFERS

7.1. **Personal Data Transfers.** Entrust agrees to allow transfer of Personal Data outside the country from which it was originally collected provided that such transfer is required in connection with the provision of Services under the Agreement and such transfers take place in accordance with the Data Protection Laws, including, without limitation, completing any prior transfer risk assessments and incorporation of a valid transfer mechanism, such as SCCs, as required by the Data Protection Laws.

Vendor is prohibited from engaging or attempting to engage in, or permitting others to engage or attempt to engage in the following: (a) selling, licensing of access to, or other similar commercial transactions, such as reselling, sub-licensing, leasing, or transferring in return for valuable consideration, the Entrust personal data including all PII or any part thereof, to countries of concern or covered persons, as defined in 28 CFR part 202; Where vendor knows or suspects that a country of concern or covered person has gained access to Entrust personal data, vendor will inform Entrust as soon as possible, and in any event no more than 48 hours after becoming aware of actual or suspected access. Failure to comply with the above will constitute a breach of the and may constitute a violation of 28 CFR Part 202. Vendor confirms that it complies with 28 CFR Part 202. Vendor agrees to periodically certify to Entrust in writing vendor's compliance with 28 CFR Part 202. Vendor agrees to not evade or avoid, cause a violation of, or attempt to violate any of the prohibitions set forth in Executive Order 14117 or 28 CFR Part 202.

7.2. **European Specific Provisions**. Where Personal Data collected in the UK, or

European Economic Area is transferred to a country outside of the European Economic Area and without an adequacy finding under Article 45 of the GDPR, whether the transfer is between Entrust and Vendor or Vendor and a third-party, at least one of the transfer mechanisms listed below shall apply:

7.2.1. **Binding Corporate Rules.** To the extent Vendor has adopted Binding Corporate Rules, it shall maintain such rules and promptly notify Entrust in the event that the rules are no longer a valid transfer mechanism between Vendor and Entrust.

7.2.2. **Standard Contractual Clauses**. The EU Standard Contractual Clauses pursuant to 2010/87/EU (the European Commission's decision 5 February 2010 and subsequently amended on June 27, 2021 (the "EU Standard Contractual Clauses"). The EU Standard Contractual Clauses are hereby incorporated in their entirety into this DPA and, to the extent applicable, Vendor shall ensure that its Sub-processors comply with the obligations of a data importer (as defined in the EU Standard Contractual Clauses). To the extent there is any conflict between this DPA and the EU Standard Contractual Clauses, the terms of the EU Standard Contractual Clauses shall prevail.

8. CERTIFICATIONS AND AUDITS

8.1. Upon written request by Entrust, Vendor, to the extent that it is acting as a Data Processor to Entrust, shall make available to Entrust all information necessary to demonstrate compliance with the obligations set forth under Data Protection Laws, provided that Vendor shall have no obligation to provide commercially confidential information. On no more than an annual basis (unless there are indications of non-compliance), Vendor shall, to the extent that it is acting as a Data Processor to Entrust, following a request by Entrust and at Entrust's expense, further allow for and contribute to audits and inspections by Entrust or its authorized third-party auditor. The scope, timing, cost and duration of any such audits, including conditions of confidentiality, shall be mutually agreed upon by Vendor and Entrust prior to initiation. Such agreement will not be unreasonably withheld or delayed by Vendor. Entrust shall promptly notify Vendor with information regarding non-compliance discovered during the course of an audit, and Vendor shall use commercially reasonable efforts to address any confirmed non-compliance.

9. NON-COMPLIANCE AND TERMINATION

9.1. **Non-compliance.** If Vendor is in breach of its obligations under this DPA, Entrust may instruct Vendor to suspend the Processing of Personal data until Vendor complies with this DPA or the contract is terminated. Vendor shall promptly inform Entrust in case it is unable to comply with this DPA, for whatever reason.

9.2. **Termination.**

9.2.1. Termination by Entrust. Entrust shall be entitled to terminate the Agreement insofar as it concerns Processing of Personal Data in accordance with this DPA if: (i) the processing of Personal Data by Vendor has been suspended by Entrust pursuant to 9.1 and if compliance with this DPA is not restored within a reasonable time and in any event within one month following suspension; (ii) Vendor is in

substantial or persistent breach of this DPA or Vendor's obligations under the Data Protection Laws, (iii) Vendor fails to comply with a binding decision of a competent court or the competent supervisory authority regarding its obligations pursuant to this DPA or the Data Protection Laws.

9.2.2. Termination by Vendor. Vendor shall be entitled to terminate the Agreement insofar as it concerns Processing of Personal Data under this DPA where, after having informed Entrust that its instructions infringe applicable legal requirements under Data Protection Laws, Entrust insists on compliance with the instructions.

10. NOTICE

10.1. Any notice required by Vendor to Entrust under this Addendum shall be sent to privacy@entrust.com.

List of Schedules

Schedule 1: Details of Personal Data Processing

Schedule 2: EU Standard Contractual Clauses

The parties' authorized signatories have duly executed this DPA:

On behalf of Vendor:

Vendor Name: _____

Name (written out in full): _____

Position: _____

Address: _____

Signature: _____

On behalf of Entrust:

Name (written out in full): **Lisa J. Tibbits**

Position: **Chief Legal and Compliance Officer**

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

Signature: 

SCHEDULE 1 – DETAILS OF PERSONAL DATA PROCESSING

When processing Personal Data on behalf of Entrust in connection with this Agreement as further detailed in Part 2 of this Schedule 1, the Vendor shall:

- keep Personal Data confidential;
- comply with Entrust's data protection policies and follow all reasonable instructions from Entrust. The Vendor shall notify Entrust immediately it if considers any of Entrust's instructions infringe the Data Protection Laws;
- not transfer any Personal Data outside of the UK or EEA or appoint any sub-Processors of the Personal Data without Entrust's prior written consent. Where Entrust agrees in writing to the appointment of a sub-Processor, the Vendor agrees to enter into a written agreement with the sub-Processor on substantially the same terms as set out in this Schedule 1 and shall remain fully liable for all acts and omissions of any such sub-Processor.
- have liability for and shall indemnity Entrust for any loss, liability, costs (including legal costs), damages or expenses resulting from any breach by the Vendor of the Data Protection Laws.

Part 2 of this Schedule 1 sets out the scope, nature and purpose of the Processing by the Vendor, the duration of the Processing and the types of Personal Data and categories of Data Subject.

PART 2 – PROCESSING PARTICULARS

Nature and Purpose of Processing

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

Duration of Processing

Vendor will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing or required by applicable law.

Categories of Data Subjects

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

For Vendors that supply a product, service or solution to Entrust for incorporation into or otherwise sold with Entrust products, services or solutions:

- Customers
- Customers’ employees, clients, agents and subcontractors

- Customer's end users authorized by Customer to use Entrust products, services or solutions

For vendors that supply a product, service or solution to Entrust personnel:

- Entrust personnel
- Customers
- Entrust suppliers or contractors

Categories of Personal Data

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

- Personal Data related to or relevant to the employment of Entrust personnel
- Business contact details of Customers, suppliers and contractors (name, title/position, address, telephone number, fax number, email address, location)
- Connection data (IP address, username, ID data used for authentication purposes)
- Any other personal data required to be processed in relation to the Services

SCHEDULE 2

EU STANDARD CONTRACTUAL CLAUSES

1 INCORPORATION OF THE EU SCCS

1.1 To the extent a transfer of Personal Data is made pursuant to the GDPR, this Schedule 2 and the following terms shall apply:

1.1.1 Module 2 of the EU SCCs, and no other optional clauses unless explicitly specified, are incorporated into this Schedule 2 as if they had been set out in full in the case where the exporter is a Controller, the importer is a Processor and the transfer requires such additional protection; and

1.1.2 Module 3 of the EU SCCs, and no other optional clauses unless explicitly specified, are incorporated into this Schedule 2 as if they had been set out in full in the case where the exporter is a Processor, the importer is a Sub-Processor and the transfer requires such additional protection.

2 CLARIFICATIONS TO THE EU SCCS

To the extent Module 2 or Module 3 of the EU SCCs applies, as determined by 1.1 of this Schedule 2 the EU SCCs shall be amended as such:

2.1 Deletion of data. For the purposes of clause 8.5 of the EU SCCs (Duration of processing and erasure or return of data), the parties agree as follows: At the end of the provision of the processing services the importer shall delete all Personal Data and shall certify to the exporter that it has done so, if requested to provide such certification by the exporter in writing.

2.2 Sub-Processors. For the purposes of clause 9 of the EU SCCs (Use of sub-processors), the parties agree that the process for appointing sub-processors set out in Schedule 1 applies.

2.3 Competent Supervisory Authority. For the purposes of clause 13 of the EU SCCs, the competent Supervisory Authority shall be:

2.3.1 if the exporter is established in an EU Member State: The Irish Data Protection Commissioner;

2.3.2 where the exporter is not established in an EU Member State and has appointed a representative pursuant to Article 27(1) GDPR, it shall notify the importer of this and the EU Member State in which the exporter's representative is appointed shall be the competent Supervisory Authority; and

2.3.3 where the exporter is not established in an EU Member State, but falls within the territorial scope of Article 3(2) GDPR but has not appointed a representative pursuant to

Article 27(1) GDPR: the exporter shall notify the importer of its chosen competent supervisory authority, which must be the Supervisory Authority of an EU Member State in which the Data Subjects whose personal data is transferred under the EU SCCs in relation to the offering of goods or services to them, or whose behaviour is monitored, are located.

2.4 Governing Law & Jurisdiction. For the purposes of clauses 17 and 18 of the EU SCCs, the parties agree that the governing law shall be where the exporter is established. If those laws do not allow for third party rights, the law of Ireland shall apply.

To the extent Module 3 of the EU SCCs applies, as determined by 1.1 of this Schedule 2 the EU SCCs shall be amended as such:

2.5 Paragraph A of Annex I to this Schedule 2 shall be modified to reflect that the exporter is a Processor and the importer is a Sub-Processor;

2.6 any request received from a data subject in connection with the personal data being processed by the importer shall be forwarded to the exporter to facilitate with the controller of such personal data; and

2.7 for the purposes of clause 8.6(c) and (d) of the EU SCCs, the importer shall notify the exporter of any personal data breach.

ANNEX I TO THE STANDARD CONTRACTUAL CLAUSES

A. List of Parties

Data exporter (Controller)

The data exporter is Entrust.

Data importer (Processor)

The data importer is the legal entity (Vendor) that has executed this DPA and as a result has accepted the Clauses as a data importer.

B. Description of Transfer Data subjects

The personal data transferred concern the following categories of data subjects:

- See Part 2, Schedule 1

Categories of data

The personal data transferred concern the following categories of data:

- See Part 2, Schedule 1

Frequency of the transfer

The personal data will be transferred on a continuous basis.

Nature and purpose of the processing

The personal data transferred will be subject to the following basic processing activities:

- The performance of the Services pursuant to the Agreement

Retention period

The personal data will be retained for the duration of the Agreement or longer if required by law.

Sub-processor transfers

The subject matter, nature and duration of processing by sub-processors is as follows:

_____

URL with list of sub-processors or add detailed list of sub- processors here.

_____

C. Competent Supervisory Authority

The supervisory authority of Ireland with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer shall act as competent supervisory authority.

ANNEX II TO THE STANDARD CONTRACTUAL CLAUSES

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

[TO BE COMPLETED BY VENDOR: *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. At a minimum, vendor must adhere to Entrust's Vendor requirements as set forth at https://www.entrust.com/legal-compliance/security*