ENTRUST CUSTOMER GLOBAL DATA PROCESSING ADDENDUM

ENTRUST ACTING AS A PROCESSOR OR SUB-PROCESSOR

Entrust and **Customer** (each as defined below) have entered into a written or electronic Agreement(s) for the purchase, access to, and/or licensing of Entrust's Services. This Data Processing Addendum ("**DPA**") supplements and forms part of the **Agreement**. Together with any additional data protection provisions contained in the Offering Schedule(s) relating to the Services, this DPA reflects the agreement of Entrust and Customer regarding the Processing of Customer Personal Data pursuant to the Agreement.

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 this DPA, the terms of the Agreement shall remain in full force and effect.

1. CUSTOMER SIGNING INSTRUCTIONS

1.1. This DPA has been pre-signed on behalf of Entrust Corporation, acting for itself and for and on behalf of each of its subsidiaries who may Process Customer Personal Data in order to provide Services pursuant to the Agreement. Unless otherwise incorporated by reference into the Agreement, to enter into this DPA, Customer must:

1.1.1. Have entered into an Agreement with Entrust;

1.1.2. Provide contact information to receive notices pertaining to this DPA by completing Clause 7, below;

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

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

2. EFFECTIVENESS

2.1. Unless otherwise incorporated by reference into the Agreement, this DPA will only be effective if executed by Customer and submitted to Entrust accurately and in full accordance with instructions in Clause 1 above. If Customer makes any deletions or other revisions to this DPA which are not explicitly agreed to by Entrust in writing, those edits to 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 - and any additional data protection provisions contained in the Offering Schedule(s) relating to the Services - shall replace any existing data processing agreement or other contractual provisions pertaining to the subject matter contained herein that the Parties may have previously entered in connection with the Services, and will be effective as of the date Entrust receives (via email to the address in Clause 1.1.4 above) a complete and executed DPA from Customer indicated in the signature block below.

2.4. **OEM Scenarios.** Where Customer makes the Services available to its own customers on an OEM, white-label, or similar basis, Schedule Three (OEM Addendum) applies and modifies this DPA solely for such OEM scenarios.

3. DEFINITIONS

"**Agreement**" means the written or electronic agreement(s) entered into between Entrust and Customer for the purchase, access to, and/or licensing of the Services.

"**BAA**" shall have the meaning given in Clause 5.3 of this DPA.

"**Biometric Data**" means data generated by automatic measurements of an individual's biological characteristics, including: (i) biometric identifiers such as a fingerprint, voiceprint, retina or iris scan, scan of a hand or face geometry, or other unique biological patterns or characteristics that is used to identify a specific individual; and (ii) any information based on an individual's biometric identifier used to identify an individual.

"**BIPA**" shall have the meaning given in Clause 5.2 of this DPA.

"**Customer Personal Data**" means Personal Data Processed by Entrust for the purpose of providing the Services to the Customer pursuant to the Agreement, as further described in Schedule 1 to this DPA (Details of Personal Data Processing).

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

"**Customer**" means a customer of Entrust Corporation (or any of its subsidiaries) who is party to the Agreement.

"**DPA**" means this Data Processing Addendum.

"**Data Protection Laws**" refers to all applicable rules, laws, regulations, directives and governmental requirements currently in effect and as they become effective relating to privacy or data protection, whether applicable at the Federal, State, or local level and including, but not limited to, the EU General Data Protection Regulation (**GDPR**), UK General Data Protection Regulation (**UK GDPR**), Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 (**e-Privacy Directive**) as transposed into applicable domestic legislation, UK's Data Protection Act 2018 (**DPA 2018**), Canada's Personal Information Protection and Electronic Documents Act (**PIPEDA**), the California Consumer Privacy Act (**CCPA**) as amended by the California Privacy Rights Act (**CPRA**), the Colorado Privacy Act (**CPA**), the Virginia Consumer Data Protection Act (**VCDPA**), the Utah Consumer Privacy Act (**UCPA**), the Connecticut Data

Privacy Act (**CTDPA**), and all biometric information privacy laws such as the Illinois Biometric Information Privacy Act (**BIPA**) (in each case, as may be amended, superseded, or replaced).

"**Data Subject**" means an identified natural person or an identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"**Entrust**" means Entrust Corporation and each of its subsidiaries who may Process Customer Personal Data to provide Services under the Agreement.

"**HIPAA**" shall have the meaning given in Clause 5.3 of this DPA.

"**OEM**" means the Customer when it makes the Services available to its own customers on an OEM, white-label, or similar basis.

"**Offering Schedule**" has the meaning given in the General Terms and Conditions. An Offering Schedule may contain additional data protection provisions regarding the Parties Processing of Customer Personal Data.

"**Parties**" means Entrust and Customer, and the term "**Party**" shall have a corresponding meaning.

"Permitted Vendor Purpose" shall have the meaning given in Clause 6.2 of this DPA.

"**Personal Data**" means any information relating to, or directly or indirectly identifying a Data Subject.

"**Personal Data Incident**" means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.

"**Processing**" (and related terms such as "**Process**", "**Processed**" and "**Processes**") means any operation or set of operations that is performed on Personal Data, whether or not by automated 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**" means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.

"**Services"** means the products, services and/or platforms provided by Entrust to Customer pursuant to, and as more fully described in, the Agreement.

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

"**Third Party Request**" shall have the meaning given in Clause 6.5 of this DPA.

"**Transfer Mechanism**" shall have the meaning given in Clause 6.9 of this DPA.

"**Ultimate Controller**" means a third-party Controller on whose behalf the OEM processes Personal Data when the OEM acts as a Processor.

"**U.S. Biometric Data Protection Laws**" means all applicable U.S. state, federal, or local laws and regulations with respect to the Processing, including collection, of Biometric Data, including

but not limited to the Illinois Biometric Information Privacy Act (**BIPA**), Texas Capture or Use of Biometric Identifier Act (**CUBI**), and Washington Biometric Law (**MHMDA**).

"**User**" means a person whose Personal Data is Processed through the Service. For example, where the purpose of the Service is to verify or authenticate a person's identity, a User is the person (who may be an employee, consumer, etc.) whose identity Customer seeks to verify or authenticate.

"**U.S. User**" shall have the meaning given in Clause 5.2 of this DPA.

4. DATA PROCESSING DETAILS

4.1. While the parties acknowledge that the characterisation of the roles of the parties is determined by Data Protection Laws, Customer and Entrust agree and acknowledge that where Customer Personal Data is Processed for the purpose of Entrust providing the Services to Customer pursuant to the Agreement, Customer is the Controller and Entrust is the Processor. Schedule 1 to this DPA (Details of Personal Data Processing) contains details of the subject matter, duration, nature and purpose of this Processing, the types of Customer Personal Data Processed, and the categories of Data Subjects concerned. In OEM scenarios, where Customer is an OEM, the Parties' roles and related obligations shall be as set out in Schedule Three (OEM Addendum).

5. CUSTOMER OBLIGATIONS

5.1. Customer shall comply with all applicable Data Protection Laws in connection with the performance of the Agreement, including by ensuring that its instructions to Entrust comply with Data Protection Laws. Customer shall provide or make available to Entrust, or assist Entrust with the collection of, Customer Personal Data, and Customer shall be solely responsible for compliance with applicable Data Protection Laws regarding the collection of, and transfer to, Entrust of Customer Personal Data. Customer represents and warrants that it has taken all required steps to ensure that Entrust may lawfully Process Customer Personal Data pursuant to the Agreement in accordance with Data Protection Laws, including having provided all necessary notices and obtained all necessary consents for Entrust to Process Customer Personal Data.

5.2. Without prejudice to Clause 5.1, to the extent Customer makes the Services available to a User who is located in, or resident of, the United States ("**U.S. User**"), Customer shall take all necessary steps to ensure that Entrust may lawfully Process U.S. Users' Personal Data - including Biometric Data - pursuant to the Agreement in accordance with U.S. Biometric Data Protection Laws. Customer shall comply with all requirements the U.S. Biometric Data Protection Laws impose regarding the provision of notice to, and the obtaining of consent from, U.S. Users. Any such notice provided by Customer must not conflict with the relevant Entrust Biometric Data Policy, available at https://www.entrust.com/legal-compliance/data-privacy.

5.3. If Customer is a "covered entity" under the Health Insurance Portability and Accountability Act ("**HIPAA**"), and Entrust will Process "protected health information" as a "business associate" as these terms are defined in 45 CFR § 160.103, execution of this DPA includes execution of the HIPAA Business Associate Agreement ("**BAA**"), the full text of which is available at https://www.entrust.com/legal-compliance/data-privacy. The BAA can only be used with those Entrust services mentioned under the "HIPAA-Covered Services" heading at https://www.entrust.com/legal-compliance/data-privacy.

6. ENTRUST OBLIGATIONS

6.1. **Instructions.** Entrust shall Process Customer Personal Data for the purposes of providing the Services to Customer in accordance with Customer's instructions as set out in the Agreement, this DPA, or in other documented instructions provided by Customer to Entrust (provided such instructions are reasonable and consistent with the terms of the Agreement). Where Entrust provides Customer with an online account or dashboard that can be used to configure the Services, the Parties agree that the choices the Customer makes in such account / dashboard shall constitute documented instructions. Entrust shall, to the extent legally permitted, inform Customer without undue delay if:

6.1.1. Entrust is required by law to Process Customer Personal Data other than in accordance with Customer's instructions. Entrust shall inform Customer of that legal requirement before commencing such Processing unless the law in question prohibits Entrust from doing so on important grounds of public interest;

6.1.2. in Entrust's opinion, a Customer instruction is in violation of Data Protection Laws; or

6.1.3. Entrust determines that it can no longer meet its obligations under Data Protection Laws in respect of the Processing of Customer Personal Data.

6.2. **Permitted Vendor Purposes.** Except for Permitted Vendor Purposes (defined below), Entrust: (a) will only retain, use, disclose, or Process Customer Personal Data obtained in the course of providing the Services on behalf of the Customer and in compliance with the Agreement; (b) will not sell or share (as defined under the CCPA) Customer Personal Data; (c) will not combine the Personal Data that it receives from Customer with other Personal Data that Entrust receives from third-party businesses (or collects from its own interaction(s) with consumers), except (i) as permitted by Customer and (ii) to perform a business purpose (as such term is defined by CCPA or its regulations); (d) will not share Customer Personal Data for the purpose of cross-contextual behavioural advertising or marketing purposes; (e) will enable Customer to take reasonable and appropriate steps as necessary to help ensure that Entrust is using the Customer Personal Data in a manner consistent with the Customer's instructions and obligations under the CCPA; (f) will not attempt to reidentify any de-

identified data; (g) will enable Customer, upon Customer's reasonable notice to Entrust, to take appropriate steps as reasonably necessary to stop and remediate any unauthorized use by Entrust of Customer Personal Data; and (h) will not take any action that would cause Entrust to cease being a "service provider" as defined under the CCPA with respect to Customer Personal Data. Entrust may, however, Process Customer Personal Data for a "business purpose" (as defined by and consistent with the CCPA) permitted of a qualified service provider under the CCPA, so long as the purpose for which the Customer Personal Data is used does not cause Entrust to lose its status as a service provider and is otherwise in compliance with all applicable Data Protection Laws ("**Permitted Vendor Purposes**").

6.3. **Authorized Personnel.** Entrust shall take measures designed to ensure the reliability of all personnel whom it instructs to Process Customer Personal Data by: (a) performing background checks upon such personnel (where permissible under applicable law); (b) assigning specific and necessity-based access privileges to such personnel; (c) ensuring that such personnel have undergone training in data protection and privacy; and (d) ensuring that such personnel are bound by obligations of confidentiality.

6.4. **Data Subject Requests.** Customer acknowledges and agrees that it is Customer's responsibility to comply with all requests from Data Subjects to whom Customer Personal Data relates, including but not limited to Data Subjects who are seeking to exercise their rights under Data Protection Laws in respect of Customer Personal Data. Where Entrust receives, from a Data Subject to whom Customer Personal Data relates, a request to exercise the rights available to them under Data Protection Laws, Entrust shall:

6.4.1. direct the Data Subject to contact Customer so that Customer may respond. For this purpose, Customer agrees that Entrust may provide such Data Subject with Customer's name and the email address provided for notices at Clause 7.1 of this DPA; and

6.4.2. upon Customer's written request, and at the Customer's reasonable expense, provide reasonable assistance as necessary to permit the Customer to respond to such requests as required by Data Protection Laws.

6.5. **Third Party Requests.** In the event Entrust directly receives any request, correspondence, inquiry, or complaint from a regulatory authority or third party which relates to Entrust's Processing of Customer Personal Data ("**Third Party Request**"), Entrust shall, to the extent legally permitted, inform Customer and provide Customer with details of such Third-Party Request. Unless legally required to do so, Entrust shall not respond to any Third-Party Request without Customer's prior consent other than to: (a) determine whether the requestor has the legal power to mandate Entrust to comply with the Third-Party Request; and/or (b) refer the requestor to the Customer.

6.6. **Privacy Assessments.** Where requested by Customer in writing and required under Data Protection Laws, Entrust shall provide such assistance as Customer reasonably requires (taking into account the nature of the Processing and the information available

to Entrust) for Customer to: (a) conduct data protection impact assessments or similar privacy assessments related to Entrust's Processing of Customer Personal Data; and (b) consult with data protection supervisory authorities regarding such assessments.

6.7. **Sub-processors.** Customer hereby provides general authorization for Entrust to engage Sub-processors to Process Customer Personal Data subject to the following requirements:

6.7.1. Entrust shall enter into a written agreement with any such Sub-processor that contains data protection obligations no less protective than those contained in this DPA.

6.7.2. Entrust shall be liable for the acts and omissions of such Sub-processor to the same extent Entrust would be liable if performing the services of the Sub-processor directly under the terms of this DPA.

6.7.3. The current list of Sub-processors who Process Customer Personal Data can be found at https://www.entrust.com/legal-compliance/data-privacy/sub-processors. Customer may request to be notified of additional or replacement Sub-processors via email by completing the "Stay Informed" form found at the above link. Customer may object to a new Sub-processor by notifying Entrust in writing within ten (10) business days of the date of Entrust's email notification. In the event Customer reasonably objects to the use of a new Sub-processor, Entrust shall use reasonable efforts to address Customer's objections. If Entrust is unable to make available such change within a reasonable period, which shall not exceed ninety (90) calendar days, Customer may terminate the Agreement with respect only to those Services which cannot be provided by Entrust without the use of the objected-to new Sub-processor by providing written notice to Entrust.

6.8. **International Data Transfers by Entrust.** Customer agrees that Entrust may transfer Customer Personal Data to a Sub-processor who will process it in a different country provided that such transfer takes place in accordance with Data Protection Laws, for example in accordance with a valid transfer mechanism such as applicable standard contractual clauses, as set forth in Schedule 2 to this DPA.

6.9. **International Data Transfers by Customer.** To the extent Customer's use of the Services requires an onward transfer mechanism to lawfully transfer Customer Personal Data from a jurisdiction (e.g., the European Economic Area, the United Kingdom or Switzerland) to Entrust's operations located outside of that jurisdiction ("**Transfer Mechanism**"), the terms set forth in Schedule 2 to this DPA (Cross Border Transfer Mechanisms) shall apply.

6.10. **Security Controls.** Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons and in accordance with its information security policies, Entrust shall establish, maintain and comply with administrative, physical, technical and organizational safeguards designed to ensure the security and confidentiality of Customer Personal

Data and to prevent the unauthorized disclosure of, or access to, Customer Personal Data. At a minimum, Entrust shall employ the security controls outlined at: https://www.entrust.com/sites/default/files/documentation/licensingandagreements/dpa-technical-and-organisational-security-measures.pdf, which Entrust reserves the right to update from time to time.

6.11. **Personal Data Incidents.** Entrust shall notify Customer without undue delay after confirming a Personal Data Incident impacting Customer Personal Data. Entrust shall take reasonable steps to identify the cause of such Personal Data Incident and take those steps reasonably necessary to remediate the cause of such a Personal Data Incident. Upon Customer's written request, Entrust shall also provide reasonable information and assistance to Customer where necessary for Customer to comply with their obligations under Articles 33 and 34 of the GDPR or equivalent provisions under Data Protection Laws.

6.12. **Certifications and audits.**

6.12.1. On no more than an annual basis and upon Customer providing sixty (60) calendar days' written notice, Entrust shall make available to Customer access to such information as is reasonably necessary for audit purposes to demonstrate Entrust's compliance with its obligations under this DPA, provided that Entrust shall have no obligation to provide confidential and/or proprietary information and all audits shall be subject to confidentiality obligations. Any audit request from Customer in excess of once per year will be at Entrust's discretion, and at Customer's sole cost (unless Customer requests such additional audit due to the previous Customer audit revealing Entrust to be in breach of Data Protection Laws). All audits are subject to confidentiality obligations.

6.12.2. In the first instance, the information Entrust shall make available to Customer to satisfy Entrust's obligation under Clause 6.12.1, will be Entrust's existing privacy and security certifications and reports, including its ISO 27701 and ISO 27001 certifications, found at https://www.entrust.com/legal-compliance/iso-certifications. If Customer demonstrates to Entrust's reasonable satisfaction that this information does not demonstrate Entrust's compliance with a particular obligation imposed on Entrust by this DPA, then Entrust shall complete a reasonable length privacy and security questionnaire to discharge its obligation under Clause 6.12.1. The questionnaire shall not exceed four (4) hours of work effort. Any questionnaire in excess of four (4) hours of work effort, or requests for documentation or artifacts (beyond Entrust's ISO 27701 and 27001 certifications or other third-party certifications shared by Entrust related to a particular service), or requests for on-site audits will be considered an audit or assessment that requires a mutually agreed upon statement of work with a charge of professional service fees to Customer. If an audit or assessment is conducted without an executed statement of work, Customer acknowledges that Entrust may still charge

back the costs of the audit to Customer. Customer shall promptly notify Entrust with information regarding non-compliance discovered during an audit and Entrust shall use commercially reasonable efforts to address any confirmed non-compliance. In addition, Customer is permitted to take reasonable and appropriate steps to stop unauthorized use of Personal Data.

6.13. **General Assistance.** Where requested by Customer in writing and required under Data Protection Laws, Entrust shall (taking into account the nature of the Processing and the information available to Entrust) provide other reasonably necessary assistance for Customer to meet its compliance obligations under Data Protection Laws with respect to the Services.

6.14. **Return or Deletion of Personal Data.** Following termination of the Agreement Entrust shall, upon Customer's written request, destroy, anonymize or return all Customer Personal Data in its possession in accordance with the procedures and timeframes specified in the relevant Offering Schedule(s) and/or product privacy notice(s) unless continued storage of Customer Personal Data is required by applicable law, or is necessary to exercise legal rights or defend legal claims. Until Customer Personal Data is destroyed, anonymized or returned, Entrust shall continue to comply with this DPA.

6.15. **Anonymized Data.** Customer Personal Data that is anonymized, de-identified, or aggregated by Entrust is not subject to this DPA; provided, however, Entrust will not re-identify or attempt to re-identify Customer Personal Data.

7. NOTICE

7.1. Any notice required by Entrust to Customer under this DPA shall be sent to _____.

7.2. If Customer has any questions regarding Processing of Customer Personal Data by Entrust, Customer may send such questions to privacy@entrust.com.

7.3. Entrust has no obligation to provide notices directly to any Ultimate Controller, as defined in Schedule three to this DPA; all notices will be provided to Customer, unless otherwise required by law, consistent with Schedule Three.

The Parties' authorized signatories have duly executed this DPA:

SIGNATURE

On behalf of Customer:

Name (written out in full): _____

Position: _____

Address: _____

Signature: _____

Date: _____

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 ONE – DETAILS OF PERSONAL DATA PROCESSING

1. **Subject Matter, Nature and Purpose of Processing**
    a. Entrust shall Process Customer Personal Data as necessary to provide the Services to Customer pursuant to the Agreement in accordance with Customer's instructions (as set out in the Agreement, this DPA, or in other documented reasonable instructions provided by Customer to Entrust where such instructions are consistent with the terms of the Agreement). See the relevant product privacy notice for more details of the Processing involved in providing each Service.

2. **Duration of Processing**
    a. Entrust shall Process Customer Personal Data for the duration of the Agreement, unless otherwise agreed upon by the Parties in writing or required by applicable law.

3. **Categories of Data Subjects**
    a. Customer determines and controls the categories of Data Subject whose Personal Data is comprised in the Customer Personal Data Processed by Entrust. The categories may include, but are not limited to, the Customer's employees, clients, agents, subcontractors and any other person whose Personal Data is Processed through the Services. See the relevant product privacy notice for more details.

4. **Categories of Customer Personal Data**
    a. Customer determines and controls the categories of Customer Personal Data Processed by Entrust which will vary depending on the Services chosen by the Customer. The categories of Personal Data may include, but are not limited to:
        i. Contact details (name, address, telephone number, email address, location).
        ii. Connection data (IP address, username, ID data used for authentication purposes).
        iii. Other categories of Personal Data specified in the relevant product privacy notice.

5. **Sensitive Data or Special Categories of Data**
    a. Customer determines and controls the categories of Personal Data Processed by Entrust which will vary depending on the Services chosen by the Customer. The categories of sensitive data or special category data may include, but are not limited to:
        i. biometric data.
        ii. Other categories of Personal Data specified in the relevant product privacy notice.

SCHEDULE TWO – CROSS BORDER DATA TRANSFER MECHANISMS

1. **Definitions**

1.1. "**EEA**" means the European Economic Area.

1.2. "**EU Standard Contractual Clauses**" mean the Standard Contractual Clauses approved by the European Commission in decision 2021/914.

1.3. "**UK International Data Transfer Agreement**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner, Version B1.0, in force 21 March 2022.

1.4. **"FADP"** means the Federal Act on Data Protection issued by The Federal Assembly of the Swiss Confederation, in force 25 September 2020.

2. Cross Border Data Transfer Mechanisms

2.1 Order of Precedence. In the event the Services are covered by more than one Transfer Mechanism, the transfer of personal data shall be subject to a single Transfer Mechanism, as applicable, and in accordance with the following order of precedence: (a) the EU Standard Contractual Clauses set forth in Section 2.2 (EU Standard Contractual Clauses) of this Schedule 2; (b) the UK International Data Transfer Agreement set forth in Section 2.3 (UK International Data Transfer Agreement) of this Schedule 2; and, if neither (a) nor (b) is applicable, then (c) other applicable data Transfer Mechanisms permitted under Data Protection Laws.

2.2 EU Standard Contractual Clauses. Module Two (Controller to Processor) of the EU Standard Contractual Clauses shall apply to personal data that is transferred via the Services from the EEA, Switzerland, Guernsey, or Jersey, either directly or via onward transfer, to any country or recipient outside the EEA, Switzerland, Guernsey, or Jersey that is not recognized by the relevant competent authority as providing an adequate level of protection for personal data. For data transfers that are subject to the EU Standard Contractual Clauses, the EU Standard Contractual Clauses shall be deemed entered into, and incorporated into this Addendum by this reference, and completed as follows:

i) in Clause 7 of the EU Standard Contractual Clauses, the optional docking clause shall not apply;
ii) in Clause 9 of the EU Standard Contractual Clauses, Option 2 shall apply and the time period for prior written notice of sub-processor changes shall be 10 calendar days;
iii) in Clause 11 of the EU Standard Contractual Clauses, the optional language shall not apply;
iv) in Clause 17 (Option 1), the EU Standard Contractual Clauses shall be governed by Irish law;

v) in Clause 18(b) of the EU Standard Contractual Clauses, disputes shall be resolved before the courts of Ireland;

vi) in Annex I, Part A of the EU Standard Contractual Clauses:

- Data Exporter: Customer
  - Contact details: The email address(es) designated by Customer in Clause 7.1 of the DPA.
  - Data Exporter Role: Controller
  - Signature and Date: By entering into the DPA, Data Exporter is deemed to have signed these EU Standard Contractual Clauses incorporated herein, including their Annexes, as of the effective date of the DPA.
  - Data Importer: Entrust Corporation and its subsidiaries.
  - Contact details: privacy@entrust.com
  - Data Importer Role: Processor
  - Signature and Date: By entering into the DPA, Data Importer is deemed to have signed these EU Standard Contractual Clauses, incorporated herein, including their Annexes, as of the effective date of the DPA.

vii) in Annex I, Part B of the EU Standard Contractual Clauses:

- The categories of data subjects are set forth in Schedule 1 (Details of Personal Data Processing) of the DPA.
- The Sensitive Data transferred is set forth in Schedule 1 (Details of Personal Data Processing) of the DPA.
- The frequency of the transfer is a continuous basis for the duration of the Agreement.
- The nature and purpose of the processing is set forth in Schedule 1 (Details of Personal Data Processing) of the DPA.
- The period for which the personal data shall be retained is set forth in Schedule 1 (Details of Personal Data Processing) of the DPA.
- For transfers to sub-processors, the subject matter, nature, and duration of the processing is set forth at https://www.entrust.com/legal-compliance/data-privacy/sub-processors

viii) in Annex I, Part C of the EU Standard Contractual Clauses: The Irish Data Protection Commission shall be the competent supervisory authority; and

ix) The security controls outlined at: https://www.entrust.com/sites/default/files/documentation/licensingandagreements/dpa-technical-and-organisational-security-measures.pdf serve as Annex II of the EU Standard Contractual Clauses.

2.3 UK International Data Transfer Agreement. Customer and Entrust agree that the UK International Data Transfer Agreement shall apply to personal data that is transferred via the Services from the United Kingdom, either directly or via onward transfer, to any country or recipient outside of the United Kingdom that is not recognized by the competent United Kingdom regulatory authority or governmental body for the United Kingdom as providing an adequate level of protection for personal data. For data transfers from the United Kingdom that are subject to the UK International Data Transfer Agreement, the UK International Data

Transfer Agreement shall be deemed entered into, and incorporated into this Addendum by this reference, and completed as follows.

i) In Table 1 of the UK International Data Transfer Agreement, Customer's and Entrust's details and key contact information are set forth in Section 2.2(vi) of this Schedule 2;

ii) In Table 2 of the UK International Data Transfer Agreement, information about the version of the Approved EU SCCs, modules, and selected clauses, which the UK International Data Transfer Agreement is appended to, are set forth in Section 2.2 (EU Standard Contractual Clauses) of this Schedule 2;

iii) In Table 3 of the UK International Data Transfer Agreement:
   (1) The list of Parties is set forth in Section 2.2(vi) of this Schedule 2.
   (2) The description of the transfer is set forth in Schedule 1 (Details of Personal Data Processing) of the DPA.
   (3) The security controls outlined at: https://www.entrust.com/sites/default/files/documentation/licensingandagreements/dpa-technical-and-organisational-security-measures.pdf serve as Annex II.

iv) The list of sub-processors is available at https://www.entrust.com/legal-compliance/data-privacy/sub-processors;

v) In Table 4 of the UK International Data Transfer Agreement, both the Importer and the Exporter may end the UK International Data Transfer Agreement in accordance with the terms of the UK International Data Transfer Agreement.

2.4 Application of EU Standard Contractual Clauses. The EU Standard Contractual Clauses apply to all Customer Personal Data that is transferred from or accessed remotely from outside any country whose data protection laws or regulations require an adequacy means for international transfer or access. The required adequacy means is met by entering into the EU Standard Contractual Clauses, either directly or via onward transfer to any country or recipient, in each case, where such transfer or access would be prohibited under Applicable Data Protection Law in the absence of the EU Standard Contractual Clauses. The EU Standard Contractual Clauses must be slightly modified (e.g., in terms of terminology) to ensure that this entire Addendum applies to all parties, regardless of the location of the parties, whether within or outside the EEA, Switzerland, Guernsey, or Jersey. Such modifications, however, do not apply for data transfers governed by EEA, Switzerland, Guernsey, or Jersey data protection laws or regulations.

2.5 Swiss Addendum to Application of EU Standard Contractual Clauses. Where the Standard Contractual Clauses apply to a transfer of Personal Data to which the FADP applies, the Standard Contractual Clauses shall be deemed to be amended to the extent necessary to operate to provide appropriate safeguards for such transfers in accordance with the FADP, including without limitation the following: (i) Clause 13(a) and Part C of Annex I are not used; the "competent supervisory authority" is the Federal Data Protection and Information Commissioner, (ii) The term "Member State" cannot be interpreted to exclude data subjects in Switzerland from exercising their rights under Data Protection Law in Switzerland; and (iii) Any amendments required from time to time by the Federal Data Protection and Information Commissioner in order to comply with the FADP.

2.6 For OEM Scenarios, where Customer acts as a Processor and Entrust acts as a Sub-processor, the Parties agree that EU SCCs Module Three (processor to processor), and the corresponding UK Addendum / Swiss adaptations apply, as set out in Schedule Three, in lieu of Module Two.

2.7 Conflict. To the extent there is any conflict or inconsistency between the EU Standard Contractual Clauses or UK International Data Transfer Agreement and any other terms in this DPA or the Agreement, the provisions of the EU Standard Contractual Clauses or UK International Data Transfer Agreement, as applicable, shall prevail.

SCHEDULE THREE – OEM ADDENDUM

This Schedule Three (the "OEM Addendum") forms part of the Entrust Customer Global Data Processing Addendum ("DPA"). This Addendum applies only where Customer makes the Services available to its own customers on an OEM, white-label, or similar basis. Capitalized terms have the meanings given in the DPA unless otherwise defined herein.

1. **Scope and Applicability.** This OEM Addendum applies where Customer ("OEM") resells, distributes, integrates, white-labels, or otherwise makes the Services available to its own customers ("Ultimate Controllers").

    1.1. This Addendum amends the DPA solely for OEM scenarios; where OEM does not act in such capacity, the DPA applies without modification.

2. **Role of the Parties.**

    2.1. OEM as Controller. Where OEM acts as a Controller, Entrust shall act as a processor in accordance with the DPA.

    2.2. OEM as Processor. Where OEM acts as a Processor on behalf of an Ultimate Controller, Entrust shall act as OEM's Sub-processor. OEM represents and warrants that it has obtained all necessary authorizations from Ultimate Controllers to appoint Entrust as a Sub-processor.

3. **Instructions and Flow-Down.**

    3.1. Entrust shall process Personal Data only on OEM's documented instructions, including any flow-down instructions of Ultimate Controllers communicated by OEM.

    3.2. In the event of conflicting instructions, OEM shall clarify the controlling instructions and. Entrust may suspend processing where necessary to avoid a violation of applicable law.

4. **Sub-processors.**

    4.1. To the extent OEM is required to notify any Ultimate Controller of Entrust's authorization or use of Sub-processors, OEM may fulfill such obligation by relying on Entrust's sub-processor notification process as described in the DPA.

    4.2. To the extent that an Ultimate Controller raises concerns regarding Entrust's use of a Sub-processor, OEM shall manage such concerns directly with the Ultimate Controller. Entrust shall have no obligation to respond to, assess, or resolve any objection made by an Ultimate Controller. OEM may raise an objection with Entrust under the objection process set out in the DPA and Entrust will address such objections in accordance with that process. If an objection raised by OEM cannot be resolved within ninety (90) days,

OEM may terminate the affected Services in accordance with the DPA.

5. **Cross-Border Data Transfers.**

   5.1. Where OEM is a Processor and Entrust is a Sub-processor, the Parties agree that EU Standard Contractual Clauses Module Three (Processor to Sub-processor) shall apply in lieu of Module Two.

   5.2. The UK Addendum and Swiss Addendum shall apply in the same manner, and the corresponding annexes will be adapted as needed to reflect the Parties' roles.

6. **Data Subject Requests.** Entrust shall direct Data Subjects to contact OEM. Entrust shall provide reasonable assistance to OEM to enable it to fulfill obligations toward Ultimate Controllers, subject to the parameters of the DPA.

7. **Personal Data Incidents.** Entrust shall notify OEM without undue delay of any Personal Data Incident affecting Ultimate Controller data. Notifications to Ultimate Controllers shall be handled by OEM unless otherwise required by law.

8. **Return or Deletion of Personal Data.** Upon termination, Entrust shall return or delete Personal Data as instructed by OEM. Where OEM acts as a Processor, OEM may instruct Entrust to return or delete data to an Ultimate Controller.

9. **Precedence.** In the event of a conflict between this Schedule Three and the remainder of the DPA, this Schedule Three controls solely OEM scenarios. Otherwise, the DPA prevails.