ENTRUST ACTING AS PROCESSOR - GLOBAL

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 (as defined below) and Customer (as defined below) for the purchase, access to, and/or licensing of products, services and/or platforms (collectively the "**Services**") to reflect the parties' agreement with regard to the Processing of Personal Data. 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. To enter into this DPA, the Customer must:

1.1.1. Have a written or electronic agreement with Entrust;

1.1.2. Complete the Customer point of contact requested in Section 9.1.

1.1.3. Complete the signature block below by providing the name of the signatory, their signature, their position, the address of the 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. 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 Customer 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 Customer indicated in the signature block below.

3. DEFINITIONS

"**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 or 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), Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) and the California Consumer Privacy Act (CCPA).

"**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.

"**Personal Data Incident**" shall have the meaning assigned in the Data Protection Laws to the terms "security incident," "security breach" or "personal data breach" and shall include any situation in which Entrust becomes aware that Personal Data has been or is likely to have been accessed, disclosed, altered, lost, destroyed or used by unauthorized persons, in an unauthorized 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.

"EU Standard Contractual Clauses" means the contractual clauses set out in Schedule 2, amended as indicated (in square brackets and italics) in Schedule 2 and as otherwise amended, superseded, or replaced from time to time in accordance with this DPA.

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

4. PERSONAL DATA PROCESSING

4.1. **Roles of the Parties**. The parties acknowledge and agree that with regard to the Processing of Personal Data under the Agreement, Customer is the Controller and Entrust is the Processor.

4.2. **Customer's Instructions for the Processing of Personal Data.** Customer's instructions for the Processing of Personal Data shall comply with Data Protection Laws. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data.

4.3. **Entrust's Processing of Personal Data**. Entrust shall only Process Personal Data on behalf of and in accordance with Customer'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 Customer where such instructions are consistent with the terms of the Agreement. Entrust shall immediately inform Customer if, in Entrust's opinion, an instruction is in violation of Data Protection Laws. For the avoidance of doubt, Entrust will not 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.

4.4. **Details of the Processing.** The subject matter of Processing of Personal Data by Entrust 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.

4.5. **Personnel**. Entrust shall 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.

4.6. **Security Controls**. Entrust 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.

4.7. **Data Subject Requests.** Entrust shall, taking into account the nature of the Processing, assist the Customer, as Data Controller, by appropriate technical and organizational measures, insofar as this is possible, in fulfilling the Customer's obligation to respond to requests from a Data Subject exercising his/her/their rights under Data Protection Laws.

4.8. **Data Protection Impact Assessment.** Entrust shall, upon Customer's written request and taking into account the nature of Processing and information available, provide reasonable assistance to Customer in connection with obligations under Articles 32 and 36 of the GDPR or equivalent provisions under Data Protection Laws.

4.9. **Return or Deletion of Personal Data.** Entrust shall, upon Customer's written request, promptly destroy, anonymize or return any Personal Data after the end of the provision of Services, unless storage of the Personal Data is required by applicable law.

4.10. **Data Processor Point of Contact**. If Customer has any questions regarding Processing of Personal Data by Entrust, Customer may send such questions to the following email: privacy@entrust.com.

5. HIPAA

5.1. 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 "HIPAA-Covered Services" as those are defined at https://www.entrust.com/legal-compliance/data-privacy. Customer may opt out of the BAA by sending the following information to privacy@entrust.com:

- the full legal name of the Customer that is opting out; and
- if Customer has multiple Agreements, the Agreement to which the opt out applies.

6. SUB-PROCESSORS

6.1. **Appointment of Sub-processors**. Customer acknowledges and agrees that Entrust may engage Sub-processors in connection with provision of the Services. Entrust 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.

6.2. **List of Current Sub-processors**. The current list of Sub-processors for the Services can be found at www.entrust.com/sub-processors.

6.3. **Notification of New Sub-processors.** Entrust will notify Customer in writing of any changes to this list of Sub-processors.

6.4. **Objection to New Sub-processors**. Customer may object to Entrust's use of a new Sub-processor by notifying Entrust in writing within ten (10) business days after receipt of Entrust's communication advising of the new Sub-processor. In the event Customer reasonably objects to the use of a new Sub-processor, Entrust will 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) days, Customer may terminate the applicable 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. Entrust 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.

6.5. **Liability.** Entrust shall be liable for the acts and omissions of its Sub-processors to the same extent Entrust 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.

7. PERSONAL DATA INCIDENTS

7.1. Entrust shall notify Customer without undue delay after becoming aware of a Personal Data Incident. Entrust shall identify the cause of such Personal Data Incident and take those steps reasonably necessary in order to remediate the cause of such a Personal Data Incident.

8. INTERNATIONAL DATA TRANFERS

8.1. **Personal Data Transfers**. Customer 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 Data Protection Laws, including, without limitation, completing any prior assessments required by Data Protection Laws.

8.2. **European Specific Provisions.** Where Entrust transfers Personal Data collected in the European Economic Area to a country outside of the European Economic Area and without an adequacy finding under Article 45 of the GDPR, Entrust shall transfer Personal Data pursuant to the EU Standard Contractual Clauses as set forth in Schedule 2. The EU Standard Contractual Clauses are hereby incorporated in their entirety into this DPA and, to the extent applicable, Entrust 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.

9. CERTIFICATIONS AND AUDITS

9.1. On no more than an annual basis and upon thirty (30) days' notice in writing by Customer, Entrust, to the extent that it is acting as a Data Processor to Customer, shall make available to Customer information necessary to demonstrate compliance with the obligations set forth under Data Protection Laws, provided that Entrust shall have no obligation to provide confidential and/or proprietary information. On no more than an annual basis and upon thirty (30) days' notice in writing, Entrust shall, to the extent that it is acting as a Data Processor to Customer, following a request by Customer and at Customer's expense, further allow for and contribute to off-site audits and inspections by Customer 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 Entrust and Customer prior to initiation. Customer shall promptly notify Entrust with information regarding non-compliance discovered during the course of an audit, and Entrust shall use commercially reasonable efforts to address any confirmed non-compliance.

10. Notice

10.1. Any notice required by Entrust to Customer under this Addendum shall be sent to _____.

List of Schedules

Schedule 1: Details of the Processing

Schedule 2: EU Standard Contractual Clauses

The parties' authorized signatories have duly executed this DPA:

On behalf of Customer:

Customer Name: _____

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 1 - DETAILS OF PERSONAL DATA PROCESSING

Nature and Purpose of Processing

Entrust 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

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

Categories of Data Subjects

Customer may submit Personal Data to Entrust, the extent of which is determined and controlled by Customer in its sole discretion (but in accordance with Data Protection Laws), and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Customer's employees, clients, agents and subcontractors
- Customer's end users authorized by Customer to use the Services
- *See also* the relevant product privacy notice

Categories of Personal Data

Customer may submit Personal Data to Entrust, the extent of which is determined and controlled by Customer in its sole discretion (but in accordance with Data Protection Laws), and which may include, but is not limited to the following categories of Personal Data:

- Business contact details (name, title/position, address, telephone number, fax number, email address, location) of Customer's employees, clients, agents, subcontractors and end users authorized by Customer to use the Services
- Connection data (IP address, username, ID data used for authentication purposes) of Customer's employees, clients, agents, subcontractors and end users authorized by Customer to use the Services
- Biometric data of Customer's employees, clients, agents, subcontractors and end users authorized by Customer to use the Services
- *See also* the relevant product privacy notice

SCHEDULE 2 – EU STANDARD CONTRACTUAL CLAUSES (Processor to Controller)

Clause 1

Purpose and scope

a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

b) The Parties:

   i. the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

   ii. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

   have agreed to these standard contractual clauses (hereinafter: "Clauses").

c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B

d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
   i. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
   ii. Clause 8.1 (b) and Clause 8.3(b);
   iii. Not used;
   iv. Not used;
   v. Clause 13;
   vi. Clause 15.1(c), (d) and (e);
   vii. Clause 16(e);
   viii. Clause 18;
b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

a) The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.
b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.
c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.
d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

8.2 Security of processing

a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data [2], the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.
b) The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.
c) The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.3 Documentation and compliance

a) The Parties shall be able to demonstrate compliance with these Clauses.

[2] This includes whether the transfer and further 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 or offences.

b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

Clause 9

Use of sub-processors

Not used.

Clause 10

Data subject rights

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

Clause 11

Redress

a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

Clause 12

Liability

a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.
c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.
e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

Clause 13

Supervision

Not used.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

The following clauses shall only apply to the extent that the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU.

a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

   i. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

   ii. the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[3];

   iii. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

[3] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative timeframe. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).
f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

The following clauses shall only apply to the extent that the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU.

15.1 Notification

a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary, with the help of the data exporter) if it:
    i. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
    ii. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much

relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

   i. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

ii. the data importer is in substantial or persistent breach of these Clauses; or
iii. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

d) Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof.] The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

Choice of forum and jurisdiction

Any dispute arising from these Clauses shall be resolved by the courts of Ireland.

ANNEX I TO THE STANDARD CONTRACTUAL CLAUSES

A. List of Parties

Data exporter

The data exporter is Customer.

Data importer

The data importer is the Entrust legal entity Customer has an Agreement with.

B. Description of Transfer

Data subjects

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

- See Schedule 1

Categories of data

The personal data transferred concern the following categories of data:

- See 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:

https://www.entrust.com/legal-compliance/data-privacy/sub-processors.

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

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

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: To the extent permitted by law, Entrust conducts background checks on all employees before employment, and employees and contractors receive information security training during onboarding as well as on an annual basis. All employees are required to read and sign Entrust's information security policies.

Compliance, audits, and certifications: Entrust, 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 governance, a set of controls and strict compliance with federal, financial, international, and industry regulations and policies. Entrust's corporate information security management system (ISMS) is ISO 27001 compliant. Additionally, Entrust maintains compliance certifications to various other standards and frameworks, depending on the product, service, and geographic location, including:

- ISO 27701
- ISO 9000
- ISO 14000
- PCI CP
- PCI SAQ
- CAIQ Cloud Security Alliance
- Webtrust – CAB Forum
- NIST/FISMA
- NIST 800-53
- ETSI
- Tscheme

To ensure that the information security strategy is effective, Entrust 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 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 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 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 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 is committed to protecting the interest of stakeholders in the event of an emergency or business disruption. Entrust 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 also maintains a Crisis Communications and Incident Response Plan to help strengthen our emergency response capability.

Business Continuity:

Entrust is committed to protecting the interest of stakeholders in the event of an emergency or business disruption. Entrust 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.

Systems and Product Acquisitions, Development and Maintenance:

Entrust's information security program includes policies, standards, and processes for System Development Lifecycle (SDLC) that are aligned with industry recognized practices for the secure management of systems throughout their lifecycle. Phases of the SDLC includes: Requirements, Design, Implementation, Testing, Deployment, Operations, Maintenance, and Retirement. . Vulnerability identification and remediation are a central focus with the goal to minimize the number of security flaws in Entrust products and services, and to minimize the impact to Customer when such flaws are discovered. The processes described herein apply to Entrust products and services and components of a partner system that may be used in conjunction with an Entrust product or service. The program will ensure that SDLC processes are consistent with Entrust information security goals and expectations. Additionally, system baselines will be established to support Entrust 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 maintains access controls and policies to manage what access is allowed to the Entrust network and systems from each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls. Entrust will maintain corrective action and incident response plans to respond to potential security threats.

Physical and Environment Security:

Entrust 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 are 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 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 accordance 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 controls as well as legal or regulatory requirements. 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.

Third-Party Management:

Entrust's third-parties, such as vendors, subcontractors, sub-processors, and service providers, that have access to data, information, facilities, or impact Entrust's products or services are continuously managed, monitored, reviewed, and bound to uphold high standards for privacy and information security. Third-parties are periodically assessed based on the sensitivity of their level of access to systems and information as well as the criticality of their services. Entrust limits access to third-parties on a "need to know" basis and revokes when it is no longer needed.