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. 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.

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 Vendor 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. DATA PROCESSOR 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.

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 unless required to do so by law to which the Vendor is subject: (i) Processing in accordance with the Agreement 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. For the avoidance of doubt, Vendor will not collect, retain, use, sell, or otherwise disclose Personal Data for any purpose other than for the specific purpose of performing the Services.

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/legal-compliance/security.

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. **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.

4.8. **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.

4.9. **Data Protection Impact Assessments.** 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.

4.10. **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.

4.11. **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.

4.12. **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: _____.

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 _____. 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.

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 TRANFERS

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 required by the Data Protection Laws.

7.2. **European Specific Provisions.** Where Personal Data collected in the European Economic Area is transferred to 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. **EU 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 (Schedule 2) 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.** In the event that 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: _____

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

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 (Controller to Processor)

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), 8.9(a), (c), (d) and (e);
   iii. Clause 9(a), (c), (d) and (e);
   iv. Clause 12(a) and (d) and (f);
   v. Clause 13;
   vi. Clause 15.1(c), (d) and (e);
   vii. Clause 16(e);
   viii. Clause 18(a) and (b);
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 importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. 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 return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all 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.

d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer 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 (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union [2] (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

i. the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
ii. the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
iii. the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
iv. the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.
c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

a) GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least thirty (30) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.
b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. [3] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.
e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

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.
b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
    i. lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
    ii. refer the dispute to the competent courts within the meaning of Clause 18.
d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

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) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.
c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) 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 and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

e) 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.

f) The Parties agree that if one Party is held liable under paragraph (e), 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.

g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

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

Clause 14

Local laws and practices affecting compliance with the Clauses

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[4];

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.

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.

[4] 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 time-frame. 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.

Clause 15

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

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 that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. 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 the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

Choice of forum and jurisdiction

a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
b) The Parties agree that those shall be the courts of Ireland.
c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
d) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX I TO THE STANDARD CONTRACTUAL CLAUSES

A. List of Parties

Data exporter

The data exporter is Entrust.

Data importer

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 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:

[TO BE COMPLETED BY VENDOR: *Add 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 organisational 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.]