DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**"), forms part of the applicable Terms of Use and/or End User License Agreement (available at www.frevvo.com/policies), or other written or electronic agreement, by and between frevvo Inc. ("**Frevvo**" or "**Processor**") and the undersigned entity (the "**Controller** ") for certain data collection and processing services (collectively, the "**Service**") provided by Processor (the "**Agreement** "). Capitalized terms not defined herein shall have the meanings ascribed to them in the Agreement. Each of Controller and Frevvo may be referred to herein as a "Party" or collectively as the "Parties" in this Addendum.

BACKGROUND

A. Controller and Processor have entered into the Agreement, which involves the Processing of Personal Data by Processor on behalf of Controller;

B. The Parties anticipate that Frevvo may process certain Personal Data outside of the European Economic Area ("**EEA**");

C. Data Protection Law requires that the Parties enter into an agreement that addresses the protection of Personal Data processed under the Agreement;

D. The Parties are entering into this Addendum to comply with the requirements set forth in Data Protection Law.

E. The Parties agree that the obligations under this DPA that are specific to the GDPR shall not apply until the GDPR has come into full force and effect.

HOW TO EXECUTE THIS DPA

1. This DPA has been pre-signed on behalf of Frevvo.
2. To complete this DPA, Controller must fill the information and sign in the appropriate boxes.
3. Frevvo will send the completed and signed DPA to Controller's email, indicating Controller's Legal Name (as set out on the applicable Order Form or Invoice, where applicable).
4. Upon receipt of the validly completed DPA by Frevvo, this DPA will become legally binding for both Parties.

HOW THIS DPA APPLIES

The Controller entity signing this DPA must be the same as the entity Party to the Agreement. If the entity signing this DPA is not a Party to the Agreement directly with Frevvo but is instead a

customer indirectly via an authorized reseller of Frevvo, this DPA is not valid and is not legally binding. Such entity should contact the authorized reseller to discuss whether any amendment to its agreement with that reseller may be required.

1. DEFINITIONS

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

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

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

"**GDPR**" means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (General Data Protection Regulation).

"**Personal Data**" means any information relating to an identified or identifiable natural person that is Processed by Processor on behalf of Controller.

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

"**Data Processor**" means the entity, including all persons operating under its supervision, which Processes Personal Data on behalf of the Controller.

"**Subprocessor**" means any processor engaged by Processor to Process Personal Data.

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

"**Control**" means in respect of a company, the power of a person to directly or indirectly secure that the affairs of the company are conducted in accordance with the wishes or directions of that person. "Controlling", "Controlled by" and "under Common Control" shall be construed accordingly.

" **Affiliate** " means, with respect to a party, any corporate entity that, directly or indirectly, Controls, is Controlled by, or is under Common Control with such party (but only for so long as such Control exists);

2. PROCESSING OF PERSONAL DATA.

2.1. Role of the Parties. The Parties acknowledge and agree that Controller is the Data Controller under the Agreement and that Processor is the Data Processor under the Agreement. Communications between the Parties related to this Addendum shall be conducted primarily by the individuals/titles described on Attachment A hereto.

2.2. Processing Instructions. Controller shall determine the scope, purposes, and manner by which the Personal Data may be accessed or processed by Processor. A description of the Processing authorized under this Addendum is set out in Attachment B hereto. Processor shall Process the Personal Data for the duration of the Agreement only as instructed in writing by Controller for the purposes authorized by Controller in accordance with this Addendum.

2.3. Compliance with GDPR. Each Party agrees to comply in their respective capacity as the Controller or Processor with applicable Data Protection Laws. Without limiting the foregoing, Processor shall:

2.3.1. Process Personal Data only on Controller's documented instructions, including transfers to third countries, unless required to do so by applicable law to which Processor is subject (and where so required Processor shall inform Controller of such requirement before Processing except where prohibited by such law);

2.3.2. Ensure that all persons authorized to Process the Personal Data are subject to contractual confidentiality obligations or are subject to corresponding appropriate statutory confidentiality obligations;

2.3.3. Take all measures required to implement appropriate technical and organizational measures to protect the security of Personal Data in accordance with applicable Data Protection Law and as appropriate in relation to applicable risks;

2.3.4. Not engage another Processor to Process Personal Data without Controller's prior written approval;

2.3.5. Provide assistance to Controller, insofar as possible and in view of the nature of the Processing, to assist controller in responding to requests of Data Subjects to exercise their rights under applicable Data Protection Law (including the GDPR);

2.3.6. Assist Controller in relation to providing security for Personal Data, data protection impact assessments, responses to breaches of Personal Data and consultations with Supervisory Authorities to

the extent required under the GDPR, taking into account the nature of the Processing and information available to Processor;

2.3.7. Promptly return or delete Personal Data at Controller's request after the termination or expiration of the Services related to Processing except where applicable law requires Processor to retain Personal Data;

2.3.8. Make available to Controller all information necessary to demonstrate its compliance with GDPR obligations and allow for and contribute to Controller's (or its agents') audits or inspections related to the Processing; Any such investigations, audits or inspections shall be upon reasonable prior written notice to controller, subject to reasonable written confidentiality terms and Processor's security requirements, limited to information relevant to Processor's compliance with this Addendum and, where feasible, not unreasonably interfere with Processor's normal business operations; and

2.3.9. In connection with clause 2.3.8 above, immediately notify the Controller if, in Processor's opinion, an instruction infringes Data Protection Law. Notwithstanding the foregoing, each Party is solely responsible for determining whether its performance of the Agreement or this Addendum is in compliance with all applicable Data Protection Laws.

2.4. Incremental Costs of Processor Assistance. The Parties acknowledge that assistance to be provided to Controller by Processor under this Addendum is not within the scope of the Agreement. In the event that assistance requested by Controller pursuant to Sections 2.3.5, 2.3.6 or 2.3.8 above require Processor to incur material, incremental costs in responding to such requests for assistance, Processor may charge Controller for, and Controller shall pay, all reasonable and documented out-of-pocket expenses incurred by Processor as well as any incremental Processor personnel time reasonably expended in responding to such requests at Processor's then standard hourly rates.

2.5. Record-Keeping. Each Party shall maintain written records of all categories of its performance and Processing activities carried out pursuant to this Addendum, including records a Party is required to maintain under applicable Data Protection Law. Each Party shall make these records available to the appropriate supervisory authority upon request.

2.6. Controller warrants that it has all of the necessary consents, permissions or other rights to lawfully provide the Personal Data to Data Processor for the Processing to be performed in relation to the Services. For avoidance of doubt, Controller is solely responsible for ensuring that all necessary Data Subject consents to this Processing are obtained and maintained in accordance with applicable Data Protection Law and for ensuring that a record of such consents is maintained.

Controller will promptly notify Processor of any required Data Subject consents which terminate, are revoked or invalidated, or expire.

3. DATA SECURITY INCIDENTS

3.1. Data Incidents.

3.1.1. If Processor becomes aware of, or reasonably suspects, a breach of the security of Personal Data, Processor shall notify Controller without undue delay.

3.1.2. Processor shall reasonably cooperate with Controller and follow Controller's reasonable instructions with regard to such incident in order to assist Controller in its investigation and response to the incident.

4. INTERNATIONAL DATA TRANSFERS

4.1. Controller acknowledges and accepts that the provision of the Service under the Agreement may require the processing of Personal Data by Subprocessors in countries outside the EEA.

4.2. To the extent that Processor transfers Personal Data out of the EEA, the Parties shall reasonably cooperate to ensure that such transfer is in compliance with Data Protection Law.

4.3. If, in the performance of this DPA, Frevvo transfers any Personal Data to a Subprocessor located outside of the EEA (without prejudice to clause 5 below), Frevvo shall in advance of any such transfer ensure that a legal mechanism to achieve adequacy in respect of that processing is in place, such as:

4.3.1. the requirement for Frevvo to execute or procure that the Subprocessor execute to the benefit of the Controller standard contractual clauses approved by the EU authorities under Data Protection Law;

4.3.2. the requirement for the Subprocessor to be certified under the EU-U.S. Privacy Shield Framework; or

4.3.3. the existence of any other specifically approved safeguard for data transfers (as recognized under Data Protection Law) and/or a European Commission finding of adequacy.

5. GENERAL AUTHORIZATION OF CERTAIN SUBPROCESSORS

5.1. Controller grants a general authorization: (a) to Frevvo to appoint third party data center operators, and outsourced marketing, business, engineering and customer support providers as Subprocessors solely to support the performance of the Service.

5.2. Frevvo has the following Subprocessors:

5.2.1. Amazon Web Services, Inc., USA Data processing activities: Various activities including storage, computation, and backup of Frevvo Service data.

5.2.2. Google, Inc., USA Data processing activities: Various activities including storage, computation, and backup of Frevvo Service data.

5.2.3. Zendesk Inc., USA Data processing activities: Various activities including storage, computation and backup of Frevvo Service data.

5.2.4. Sendgrid Inc., USA Data processing activities: Various activities including storage, computation and backup of Frevvo Service data.

5.3. If Controller has a reasonable objection to any new or replacement Subprocessor, it shall notify Frevvo of such objections in writing within ten (10) days of the notification by Frevvo of its intention to appoint such new or replacement Subprocessor and the Parties will seek to resolve the matter in good faith. If Frevvo is reasonably able to provide the Service to the Controller in accordance with the Agreement without using the Subprocessor and decides in its discretion to do so, then the Controller will have no further rights under this clause 5 in respect of the proposed use of the Subprocessor. If Frevvo requires use of the Subprocessor in its discretion and is unable to satisfy the Controller as to the suitability of the Subprocessor or the documentation and protections in place between Frevvo and the Subprocessor within thirty (30) days from the Controller's notification of objections, the Controller may within thirty (30) days following the end of the thirty (30) day period referred to above, terminate the applicable Order Form and/or Insertion Orders with at least thirty (30) days written notice, solely with respect to the service(s) to which the proposed new Subprocessor's processing of Personal Data relates. If the Controller does not provide a timely objection to any new or replacement Subprocessor in accordance with this clause 5.3, the Controller will be deemed to have consented to the Subprocessor and waived its right to object to such Subprocessor. If Processor engages a Subprocessor to carry out Processing activities on behalf of Controller, Processor shall require the Subprocessor to execute a written agreement to adhere to the same obligations that are imposed on Processor in this Addendum. Processor acknowledges that it shall remain fully liable to Controller for the performance of the Subprocessor's obligations.

INDEMNIFICATION; LIMITS OF LIABILITY

Processor agrees to indemnify, defend, and hold harmless Controller against all claims, actions, third party claims, losses, damages and expenses incurred by Controller and arising directly or indirectly out of or in connection with a breach of this Addendum and/or Data Protection Law by Processor. Controller agrees to indemnify, defend, and hold harmless Processor against all claims, actions, third party claims, losses, damages and expenses incurred by Processor and arising directly or indirectly out of or in connection with a breach of this Addendum and/or the Data Protection Law by Controller. Under no circumstances will either Party's liability under this Agreement include any claims or losses for indirect, consequential, special or punitive

damages, including without limitation loss of profits, business opportunity, or data, regardless of whether a Party knew or should have known of the possibility of such loss or damages to the other Party. Except as may be required to comply with a fully-adjudicated order of a Supervisory Authority or competent court of law in the European Union or a Member Country thereof, neither Party's total liability to the under this Agreement shall exceed the amounts paid or payable to Processor by Controller under the Agreement.

TERM

This Addendum shall expire on the termination or expiration of the Agreement, or, if earlier, upon the cessation of all Processing by Frevvo pursuant to the Agreement.

ENTIRE AGREEMENT; CONFLICT

This Addendum supersedes and replaces all prior and contemporaneous proposals, statements, sales materials or presentations and agreements, oral and written, with regard to the subject matter of this Addendum, including any prior data processing addenda entered into between Processor and Controller. If there is any conflict between this Addendum and any agreement, including the Agreement, the terms of this Addendum shall control.

This Addendum and any action related thereto shall be governed by and construed in accordance with the laws of the State of Connecticut, USA, without regard to that body of law applicable to conflicts of laws. The parties consent to the personal jurisdiction of, and venue in, the courts of the County of New Haven, Connecticut.

This Data Protection Agreement, Attachment A, Attachment B, the EU Standard Contractual Clauses, Appendix 1 to the EU Standard Contractual Clauses, and Appendix 2 the EU Standard Contractual Clauses, attached thereto are hereby acknowledged and agreed by each party's authorized representative.

Controller

Entity Name: _____

By: _____

Name: _____

Title: _____

Date: _____

Processor

Entity Name: frevvo Inc._____

By: _____

Name: Ashish Deshpande_____

Title: CEO_____

Date: May 15, 2018_____

Attachment A

Contact information of the Data Protection Officer of the Data Controller.

Name: _____

Email: _____

Contact information of the Data Protection Officer of the Data Processor.

Name: Yuri de Wit

Email: yuri.dewit@frevvo.com

Attachment B
Details of Personal Data and Processing Activities

1. The Personal Data comprises: in relation to visitors of the Controller's online properties identification data, professional life data, personal life data, connection data, or localization data (including IP addresses). Controller, its online visitors and/or other partners may also upload content to Controller's online properties which may include Personal Data and special categories of data, the extent of which is determined and controlled by the Controller in its sole discretion. Such special categories of data include, but may not be limited to, information revealing racial or ethnic origins, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning an individual's health or sexual and gender orientation.

2. The duration of the processing will be: until the earliest of

   2.1. expiry/termination of the Agreement, or

   2.2. the date upon which processing is no longer necessary for the purposes of either Party performing its obligations under the Agreement (to the extent applicable);

3. The processing will comprise: Processing necessary to provide the Service to Controller, pursuant to the Agreement;

4. The purpose(s) of the processing is/ are: necessary for the provision of the Service;

5. Personal Data may concern the following data subjects:

   5.1. Prospective customers, customers, resellers, referrers, business partners, and vendors of the Controller (who are natural persons);

   5.2. Employees or contact persons of the Controller's prospective customers, customers, resellers, referrers, Subprocessors, business partners, and vendors (who are natural persons);

   5.3. Employees, agents, advisors, and freelancers of the Controller (who are natural persons); and/or

   5.4. Natural persons authorized by the Controller to use the Service.

EU STANDARD CONTRACTUAL CLAUSES

INTRODUCTION

Both Parties have agreed on the following Contractual Clauses (the " **Clauses** ") in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the Personal Data specified in Appendix 1.

AGREED TERMS

1) **DEFINITIONS**. For the purposes of the Clauses:
   a) **'Personal Data'**, '**special categories of data'**, '**process/processing'**, '**controller'**, '**processor'**, '**data subject'** and '**supervisory authority'** shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of Personal Data and on the free movement of such data;
   b) **"the data exporter"** shall mean the controller who transfers the Personal Data;
   c) **"the data importer"** shall mean the processor who agrees to receive from the data exporter Personal Data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of these Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
   d) **"the Subprocessor"** means any processor engaged by the data importer or by any other Subprocessor of the data importer who agrees to receive from the data importer or from any other Subprocessor of the data importer Personal Data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
   e) **"the applicable data protection law"** means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of Personal Data applicable to a data controller in the Member State in which the data exporter is established;
   f) **"technical and organizational security measures"** means those measures aimed at protecting Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.
2) **DETAILS OF THE TRANSFER.** The details of the transfer and in particular the special categories of Personal Data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.
3) **THIRD-PARTY BENEFICIARY CLAUSE**

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the Subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the Subprocessor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

4) **OBLIGATIONS OF THE DATA EXPORTER.** The data exporter agrees and warrants:

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

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

c) that the data importer will provide sufficient guarantees in respect of the technical and organizational security measures specified in Appendix 2 to these Clauses;

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

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

f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be

transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

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

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

i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a Subprocessor providing at least the same level of protection for the Personal Data and the rights of data subject as the data importer under the Clauses; and

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

5) **OBLIGATIONS OF THE DATA IMPORTER.** The data importer agrees and warrants:

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

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

c) that it has implemented the technical and organizational security measures specified in Appendix 2 before processing the Personal Data transferred;

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

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

ii) any accidental or unauthorized access; and

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

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

f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data

exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

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

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

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

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

6) **LIABILITY**

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

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

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

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

7) **MEDIATION AND JURISDICTION**

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
    a. to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
    b. to refer the dispute to the courts in the Member State in which the data exporter is established.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

8) **COOPERATION WITH SUPERVISORY AUTHORITIES**

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any Subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any Subprocessor preventing the conduct of an audit of the data importer, or any Subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

9) **GOVERNING LAW.** The Clauses shall be governed by the law of the Member State in which the data exporter is established.

10) **VARIATION OF THE CONTRACT.** The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clauses.

11) **SUB-PROCESSING**

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the Subprocessor which imposes the same obligations on the Subprocessor as are imposed on the data importer under the Clauses. Where the Subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the Subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the Subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such

third-party liability of the Subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

12) **OBLIGATION AFTER THE TERMINATION OF PERSONAL DATA-PROCESSING SERVICES**

1. The parties agree that on the termination of the provision of data processing services, the data importer and the Subprocessor shall, at the choice of the data exporter, return all the Personal Data transferred and the copies thereof to the data exporter or shall destroy all the Personal Data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the Personal Data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the Personal Data transferred and will not actively process the Personal Data transferred anymore.
2. The data importer and the Subprocessor warrant that upon the request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses. The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

DATA EXPORTER. The data exporter is (i) the legal entity that has executed the Agreement with Frevvo and (ii) all affiliates of such entity established within the EEA, which have purchased services from Frevvo or its Affiliates. The data exporter has appointed the data importer to provide the Service as specified in the Agreement. To facilitate the provision of the Service, the data exporter may provide to the data importer access to the Personal Data described below.

DATA IMPORTER. The data importer is Frevvo which provides the Service. The data importer will be the recipient of Personal Data which is exported by the data exporter to the data importer as described below.

DATA SUBJECTS. The Personal Data transferred may concern the following categories of data subjects: The data exporter may submit Personal Data to Frevvo and its Affiliates, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Prospective customers, customers, resellers, referrers, business partners, and vendors of the data exporter (who are natural persons);
- Employees or contact persons of the data exporter's prospective customers, customers, resellers, referrers, subcontractors, business partners, and vendors (who are natural persons);
- Employees, agents, advisors, and freelancers of the data exporter (who are natural persons); and/or
- Natural persons authorized by the data exporter to use the services provided by Frevvo to the data exporter.

CATEGORIES OF DATA. The data subjects' Personal Data transferred may concern the following categories of data The data exporter may submit Personal Data to Frevvo and its Affiliates, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to, the following categories of Personal Data:

- Names, titles, position, employer, contact information (email, phone, fax, physical address etc.), identification data, professional life data, personal life data, connection data, or localization data (including IP addresses).

SPECIAL CATEGORIES OF DATA (IF APPROPRIATE). The data exporter may submit special categories of data to Frevvo and its Affiliates, the extent of which is determined and controlled by the data exporter in its sole discretion. Such special categories of data include, but may not be limited to, Personal Data with information revealing racial or ethnic origins, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning an individual's health or sexual and gender orientation.

PROCESSING OPERATIONS. The Personal Data transferred may be subject to the following processing activities: The objective of the processing of Personal Data by Frevvo is to provide the Service, pursuant to the Agreement.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses.

Data Importer Information Security Overview

1. Data importer/Subprocessor has implemented and shall maintain a security program in accordance with industry standards.
2. More specifically, data importer/Subprocessor's security program shall include:

Access Control of Processing Areas

Data importer/Subprocessor implements suitable measures in order to prevent unauthorized persons from gaining physical access to the data processing equipment (such as database and application servers and related hardware) where the Personal Data are processed or used, including:

- establishing security areas
- protection and restriction of access paths;
- establishing access authorizations for employees and third parties, including the respective documentation;
- all access to the data center where Personal Data are hosted is logged, monitored, and tracked; and
- the data center where Personal Data are hosted is secured by appropriate security measures.

Access Control to Data Processing Systems

Data importer/Subprocessor implements suitable measures to prevent their data processing systems from being used by unauthorized persons, including:

- use of adequate encryption technologies;
- identification of the terminal and/or the terminal user to the data importer/Subprocessor and processing systems;
- automatic temporary lock-out of user terminal if left idle, identification and password required to reopen;
- automatic temporary lock-out of the user ID when several erroneous passwords are entered, log file of events, monitoring of break-in-attempts (alerts); and
- all access to data content is logged, monitored, and tracked.

Access Control to Use Specific Areas of Data Processing Systems

Data importer/Subprocessor commits that the persons entitled to use their data processing system are only able to access the data within the scope and to the extent covered by their respective access permission (authorization) and that Personal Data cannot be read, copied or modified or removed without authorization. This shall be accomplished by various measures including:

- employee policies and training in respect of each employee's access rights to the Personal Data;
- allocation of individual terminals and/or terminal user, and identification characteristics exclusive to specific functions;

- monitoring capability in respect of individuals who delete, add or modify the Personal Data;
- release of data only to authorized persons.

Availability Control

Data importer/Subprocessor implements suitable measures to ensure that Personal Data are protected from accidental destruction or loss, including:

- infrastructure redundancy;
- backup is stored at an alternative site and available for restore in case of failure of the primary system.

Transmission Control

Data importer/Subprocessor implements suitable measures to prevent the Personal Data from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the data media. This is accomplished by various measures including:

- use of adequate firewall, VPN and encryption technologies to protect the gateways and pipelines through which the data travels; and
- as far as possible, all data transmissions are logged, monitored and tracked.

Input Control

Data importer/Subprocessor implements suitable input control measures, including:

- an authorization policy for the input, reading, alteration and deletion of data;
- authentication of the authorized personnel;
- utilization of unique authentication credentials or codes (passwords);
- providing that entries to data processing facilities (the rooms housing the computer hardware and related equipment) are kept locked;
- automatic log-off of user ID's that have not been used for a substantial period of time.

Separation of Processing for different Purposes

Data importer/Subprocessor implements suitable measures to ensure that data collected for different purposes can be processed separately, including:

- access to data is separated through application security for the appropriate users;
- modules within the data importer/Subprocessor's database separate which data is used for which purpose, i.e. by functionality and function;
- at the database level, data is stored in different normalized tables, separated per module, per Controller or function they support;
- interfaces, batch processes and reports are designed for only specific purposes and functions, so data collected for specific purposes is processed separately.

Documentation

Data importer/Subprocessor will keep documentation of technical and organizational measures in case of audits and for the conservation of evidence. Data importer/Subprocessor shall take reasonable steps to ensure that persons employed by it, and other persons at the place of work concerned, are aware of and comply with the technical and organizational measures set forth in this Appendix.

Monitoring

Data importer/Subprocessor shall implement suitable measures to monitor access restrictions to data importer/Subprocessor's system administrators and to ensure that they act in accordance with instructions received. This is accomplished by various measures including:

- individual appointment of system administrators;
- adoption of suitable measures to register system administrators' access logs to the infrastructure and keep them secure, accurate and unmodified for at least six months;
- yearly audits of system administrators' activity to assess compliance with assigned tasks, the instructions received by the data importer/Subprocessor and applicable laws;
- keeping an updated list with system administrators' identification details (e.g. name, surname, function or organizational area) and tasks assigned and providing it promptly to data exporter upon request.