# Data Processing Addendum

1. **DEFINITIONS.** Capitalized terms used and not defined in this Data Processing Addendum have the respective meanings assigned to them in the main body of the Agreement.

“**Applicable Law**” shall mean all regional, national, and international laws, rules, regulations, and standards including those imposed by any governmental or regulatory authority which apply from time to time to the person or activity in the circumstances in question.

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

“**Data Privacy Law**” means, any Applicable Law or regulation relating to the protection of Personal Data, including, without limitation, the EU General Data Protection Regulation 2016/679, and the implementing acts of the foregoing by the member state of the European Union and/or the European Economic Area (collectively, the “**GDPR**”), and the California Consumer Privacy Act of 2018 (the “**CCPA**”).

“**Data Subject**” means an identified or identifiable individual who is the subject of Personal Data, the Processing of which is governed under applicable Data Privacy Law. The term “Data Subject” also includes the term “customer” as defined under the CCPA.

“**Personal Data**” any Personal Information (as defined in the main body of the Agreement) Processed by Eved on behalf of Customer, including, without limitation, the term “personal data” as defined under the GDPR and the term “personal information” as defined under the CCPA.

“**Processing**” means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether through automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure or destruction. “**Process**” and “**Processed**” have correlative meanings.

“**Processor**” means a natural or legal person, public authority, agency, or other body which Processes Personal Data on behalf of a Controller.

“**Subprocessor**” means a third party engaged by Eved to assist with the provision of the Services which involves the Processing of Personal Data.

2. **STATUS OF PARTIES.** The parties acknowledge and agree that with regard to the Processing of Personal Data, Customer is the Controller under GDPR and the business under CCPA and Eved is the Processor under GDPR and the Eved under CCPA.

3. **SCOPE OF DATA PROCESSING.** Eved will Process the Personal Data during the Term as set forth in Appendix 1 to the Standard Contractual Clauses. The parties agree and acknowledge that the disclosure of Personal Data to Eved is for a business purpose (as defined under the CCPA) and such disclosure is not made for any monetary or other valuable consideration.

4. **PROCESSOR OBLIGATIONS.**

4.1. Eved will Process the Personal Data only in accordance with any written Customer instructions received by Eved with respect to the Processing of such Personal Data and in a manner necessary for the provision of the Services by Eved which includes, without limitation, all Processing in accordance with this DPA and the main body of the Agreement. Customer’s instructions shall be issued in writing or via e-mail. Eved shall not use or otherwise disclose or make available any Personal Data for Eved’s own purposes without Customer’s prior written consent.

4.2. In the event Eved is required under any Applicable Law to Process Personal Data in excess of Customer’s documented instructions, Eved shall immediately notify Customer of such a requirement, unless such Applicable Law prohibits such notification on important grounds of public interest, in which case it will notify Customer as soon as the Applicable Law permits it to do so.

4.3. Eved shall promptly notify Customer if Eved reasonably believes that an instruction issued Customer would violate any Data Privacy Laws.

4.4. Taking into account the nature of the Processing, Eved shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure, data portability, objection to the Processing, or its right not to be subject to an automated individual decision making made under applicable Data Privacy Law (“**Data Subject Request**”). Eved shall, to the extent legally permitted, promptly notify Customer if Eved receives a Data Subject Request. Eved shall not respond to a Data Subject Request except on the document instructions of Customer or as required under Applicable Law. To the extent legally permitted, Customer shall be responsible for any costs arising from Eved's performance under this Section 4.4.

4.5. Eved shall, to the extent specifically required under applicable Data Privacy Law, assist Customer in complying with its obligations with respect to Personal Data including, without limitation, the obligations set forth in Articles 32 to 36 of the GDPR.

4.6. Eved will ensure that persons authorized to Process Personal Data on behalf of Eved have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

4.7. Eved shall not disclose the information to a third party for monetary or other valuable consideration.

## 5. CUSTOMER PROCESSING.

5.1. **Customer Processing.** Customer will, in its use of the Services, Process Personal Data in accordance with the requirements of applicable Data Privacy Laws. Customer's instructions to Eved for the Processing of Personal Data will comply with Data Privacy Laws and Customer will have sole responsibility for the creation, collection, receipt, transmission, storage, access, disposal, use, and disclosure of any Personal Information acquired by Customer or by Eved on Customer’s behalf and for the accuracy, quality, and legality of such Personal Data and the means by which Customer acquired such Personal Data. Customer shall be solely responsible for the unauthorized creation, collection, receipt, transmission, access, storage, disposal, use, or disclosure of Personal Information under its control or possession.

5.2. **Personal Data from EU and/or Switzerland.** With respect to Personal Data originating in the EEA and Switzerland, if required under applicable data protection law, prior to making any such Personal Data available to Eved, directly or through the Services, Customer shall obtain consents from all Data Subjects whose Personal Data may be Processed by the Services to the transfer of such Personal Data to the United States or other countries and to the Processing of such Personal Data for the purposes described in this DPA and the main body of the Agreement. Customer shall also obtain all authorizations and give all notices to data protection authorities within the EEA and Switzerland that are required by applicable Data Privacy Laws prior to the Processing of such Personal Data to Eved.

5.3. **Personal Data from Other Jurisdictions.** With respect to Personal Data originating in any other jurisdiction, Customer shall obtain all consents and take all other actions required under applicable Data Privacy Laws to make the transfer and Processing of such Personal Data as contemplated in this DPA and the main body of the Agreement fully consistent with the requirements of the Applicable Laws of the jurisdiction where such Personal Data originated.

**6.** **PROCESSING INSTRUCTIONS.** Customer instructs Eved to Process Personal Data for the following purposes: (a) as necessary for the provision of the Services and in accordance with the main body of the Agreement; (b) as necessary for Processing initiated by Data Subjects in their use of the Services; and (c) as necessary to comply with the other reasonable instructions provided by Customer to Eved (e.g., via email or via support requests) where such instructions are consistent with the terms of the main body of the Agreement. Customer further instructs Eved to Process Personal Data pursuant to data analytics or monitoring carried out by Eved in connection with the provision of Services or otherwise connected with Customer's use of the Services. Customer further instructs Eved that it may aggregate, deidentify, or anonymize Personal Data ("**Aggregated Data**") such that it is no longer considered Personal Data and use such Aggregated Data for its own purposes.

**7.** **SECURITY.**

7.1. **Security Measures.** Taking into account the state of the art, costs of implementation, and nature, scope, context, and purposes of the Processing as well as the risk of varying likelihood and severity for the rights and freedoms of Data Subjects, the Eved shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, as further set forth in Appendix 2 of the Standard Contractual Clauses.

7.2. **Security Incident Notification.** If Eved becomes aware of any unauthorized or unlawful access to, or acquisition, alteration, use, disclosure, or destruction of, Customer's Personal Data, including any "personal data breach" as defined in the GDPR ("**Security Incident**"), Eved will notify Customer without undue delay after becoming aware of the Security Incident. Eved will also reasonably cooperate with Customer with respect to any investigations and with preparing potentially required notices, and provide any information reasonably requested by Customer in relation to the Security Incident.

**8.** **SUBPROCESSORS.** Customer hereby provides a general authorization to Eved to Subprocessors, subject to compliance with the requirements in this Section. Eved will: (b) ensure that all Subprocessors are bound by contractual terms no less onerous than those contained in this DPA; and (b) be liable for the acts and omissions of its Subprocessors to the same extent Eved would be liable if performing the portion of the Services performed of each of those Subprocessors directly under the terms of this DPA, except as otherwise set forth in the main body of the Agreement. Eved will provide Customer with an opportunity to object to any addition or replacement of any Subprocessor.

**9.** **INTERNATIONAL DATA TRANSFERS.** The Standard Contractual Clauses attached hereto as Attachment 1 will apply to all Processing of Personal Data by Eved where the Personal Data is transferred from the European Economic Area ("**EEA**") to outside the EEA from the a data exporter acting as a Controller and a data importer acting as a Processor, to any country or recipient: (a) not recognized by the European Commission as providing an adequate level of protection for Personal Data (as described in the applicable Data Privacy Law), and (b) not covered by a suitable framework recognized by the relevant authorities or courts as providing an adequate level of protection for Personal Data.

## 10. RETURN AND DESTRUCTION.

10.1. Without prejudice to any obligations under this Section 10, following termination or expiration of the Agreement for whatever reason, Eved shall, and shall all Subprocessors to, cease Processing Personal Data.

10.2. Following termination or expiration of the Agreement for whatever reason and having received written confirmation from Customer, Eved shall destroy all copies of Personal Data, unless and for the duration Eved is permitted to retain such Personal Data in accordance with Applicable Laws. Notwithstanding the foregoing, to the extent it is not commercially reasonable for Eved to remove Personal Data from archive or other backup media, Eved may retain Personal Data on such media in accordance with its backup or other disaster recovery procedures. In the event Eved retains Personal Data after the Term, Eved shall continue to comply with the confidentiality and privacy obligations hereunder until it is no longer in possession of Personal Data.

10.3. To the extent feasible, Eved shall archive documentation that is evidence of proper Processing of Personal Data beyond termination or expiration of the Agreement and continuing for any period of time in which Eved retains Personal Data.

## 11. AUDITS.

11.1. Eved shall, upon receiving at least thirty (30) days prior written notice from Customer, submit or procure that its Subprocessors submit (as requested), its or their data Processing facilities for a reasonable audit of Processing activities carried out under this DPA, where such audit shall be carried out by an independent third-party auditor mutually agreed upon by the parties and bound by a duty of confidentiality ("**Auditor**") and, where applicable, approved by the relevant supervisory authority. Any effort as well as internal and external costs of audits requested by Customer pursuant to this Section 11 shall be borne by Customer.

11.2. Eved shall provide Customer or Auditor with the necessary information and shall keep the necessary records required for an audit of the Processing of Personal Data and will, subject to Applicable Law, provide said documents and/or data media to Customer upon written request. Eved shall provide reasonable support for any and all audits of Customer or Auditor under this Section 11 and shall contribute to the complete and efficient completion of the audit.

## 12. MISCELLANEOUS.

12.1. **Liability.** Any claims brought under this DPA will be subject to the same terms and conditions, including the exclusions and limitations of liability, as set out in the main body of the Agreement. Eved's liability to Customer under this DPA will be limited to the same extent as Eved's liability to Customer under the main body of the Agreement. In no event will any party limit its liability with respect to any Data Subject rights under the Standard Contractual Clauses.

12.2. **Governing Law.** Without prejudice to Clause 7 and Clause 9 of the Standard Contractual Clauses: (a) the parties to this DPA hereby subject to the choice of jurisdiction stipulated in the main body of the Agreement with respect to any disputes or claims howsoever arising under this DPA, including disputes regarding its existence, validity, or termination or the consequences of its nullity; and (b) this DPA and all non-contractual or other obligations arising out of in connection with it are governed by the laws of the country, territory, or jurisdiction stipulated for this purpose in the main body of the Agreement.

12.3. **Changes in Data Protection Legislation.** Both Eved and Customer may: (a) by at least 30 (thirty) days' written notice to the other party from time to time make any variations to this DPA, which are required as a result of any change in, or decision of a competent authority under, that Data Privacy Laws, to allow such Processing to be done (or continue to be done) without breach of such Data Privacy Laws; and (b) propose any other variation to this DPA which either party reasonably considers to be necessary to address the requirements of any Data Privacy Laws.

12.4. **Counterparts.** This DPA may be executed in counterparts, each of which shall be deemed an original, but all of which together shall be deemed to be one and the same document. The signatures of all the parties do not need to be on the same counterpart for it to be effective. Delivery of an executed counterpart's signature page of this DPA, by facsimile, electronic mail in portable document format (.pdf) or by any other electronic means intended to preserve the original graphic and pictorial appearance of a document, has the same effect as delivery of an executed original of this DPA.

12.5. **Severability.** If any provision of this DPA is invalid, illegal, or unenforceable by any court or administrative body of competent jurisdiction, such invalidity, illegality, or unenforceability shall not affect any other term or provision of this DPA and all such other terms and provisions shall remain in full force and effect.

12.6. **Entire Agreement.** This DPA, together with the Standard Contractual Clauses and the main body of the Agreement, constitutes the sole and entire agreement of the parties with respect to the subject matter of this DPA, and supersedes all prior and contemporaneous understandings, agreements, representations, and warranties, both written and oral, with respect to the subject matter. In the event of any inconsistency between the statements in this DPA, the main body of the Agreement, and the Standard Contractual Clauses, the following order of precedence governs: (a) the Standard Contractual Clauses; (b) this DPA; and (c) the main body of the Agreement. Subject to the foregoing, all other provisions of the main body of the Agreement apply.

12.7. **Headings.** The headings in this DPA are for reference only and shall not affect the interpretation of this DPA.

## Attachment 1 to the DPA

## Commission Decision C(2010)593
## Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

These clauses supplement the Software as a Service Agreement between the party as set forth therein into which these clauses are incorporated hereinafter "**data exporter**"

And

Name of the data importing organisation: Eved LLC

Address: 350 W. Ontario Street, 6th Floor; Chicago, Ill. 60654; USA

e-mail: finance@eved.com

Other information needed to identify the organisation:

N/A
(the "**data importer**")

each a "party"; together "the 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.

## *Clause 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'* means the controller who transfers the personal data;

(c) *'the data importer'* means 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 the 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 organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

## *Clause 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.

## *Clause 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.

## *Clause 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 organisational security measures specified in Appendix 2 to this contract;

(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, unauthorised 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 subprocessing 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 subprocessing, 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).

*Clause 5*

### *Obligations of the data importer*[1]

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 organisational 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 unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised 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

[1] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia*, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

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 subprocessing, 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 subprocessing, 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;

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

### *Clause 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 of 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.

### *Clause 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.

*Clause 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).

*Clause 9*

### *Governing Law*

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

*Clause 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 Clause.

*Clause 11*

### *Subprocessing*

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[2].

[2] This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.

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 subprocessing 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 subprocessing 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.

## *Clause 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 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 and must be completed and signed by the parties.
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 (please specify briefly your activities relevant to the transfer):

*Is a seller of goods and services to buyers who plan and manage events through the data importer's services.*

**Data importer**
The data importer is (please specify briefly activities relevant to the transfer):

*Data importer provides an event planning service that allows event planners to manage event spending and to connect with potential providers of event services and to facilitate, enter into, and manage transactions related to planned events. Personal Data is used to connect the buyers and sellers and to facilitate the processing of transactions conducted on or through the data importer's service, including the processing of payment between the buyer's and seller's organizations.*

**Data subjects**
The personal data transferred concern the following categories of data subjects (please specify):

*Employees of buyers and selers who use the data importer's services.*

**Categories of data**
The personal data transferred concern the following categories of data (please specify):

*Contact information of buyers and sellers and their respective employees: name, address, phone number, employee ID, business division/department name. Also includes a customer's employee's chosen user name, password, and (optionally) photograph.*

**Special categories of data (if appropriate)**
The personal data transferred concern the following special categories of data (please specify):

*None*

**Processing operations**
The personal data transferred will be subject to the following basic processing activities (please specify):

*Collection, recording, organization, structuring, storage, adaption and alteration, retrieval, consultation, use, disclosure by transmission, dissemination, and making available personal data (described above) for the data subjects and purposes described above.*

## APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

**Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):**

1. **DEFINITIONS.** Capitalized terms used herein shall have the meanings ascribed to them in the main body of the Agreement to which this Exhibit is attached to, this Exhibit B, or as otherwise defined below.

"**Authorized Representatives**" means Eved's Representatives who have a need to know or otherwise access Customer Data to enable Eved to perform its obligations under the Agreement and this Exhibit, and who are bound in writing by confidentiality and other obligations sufficient to protect Customer Data in accordance with the terms and conditions of the Agreement and this Exhibit.

"**AWS**" has the meaning set forth in Section 2.1.

"**Compliance Resources**" has the meaning set forth in Section 2.1.

"**PCI DSS**" has the meaning set forth in Section 3.4.

"**Security Incident**" means a breach of security leading to the accidental, unlawful, or unauthorized destruction, loss, alteration, or disclosure of, or access to, Customer Data transmitted, stored, or otherwise processed by Eved.

2. **STANDARD OF CARE.**

2.1. **<u>Hosting by Amazon Web Services</u>.** Customer acknowledges and understands that the Hosted Services are hosted by Amazon Web Services, Inc. ("**AWS**"), a third-party Eved. Customer further acknowledge and agrees that Eved has no control over AWS's environment or how AWS maintains its environment. Accordingly, the requirements set forth in this Exhibit shall only apply to Eved's internal infrastructure and the subscribed AWS service offerings which constitute the cloud infrastructure that hosts the Hosted Services (solely to the extent Eved can modify, alter, or otherwise define the configuration of such cloud infrastructure). The Parties acknowledge and agree that AWS makes certain representations regarding its security processes and procedures (as generally available at https://aws.amazon.com/security), and that Customer has reviewed, understood, and approved of such security processes and procedures. Customer may, at any time, verify AWS' compliance by going to the following webpages: https://d1.awsstatic.com/whitepapers/security/AWS_Security_Whitepaper.pdf and https://aws.amazon.com/compliance/ ("**Compliance Resources**"). The Compliance Resources are available to Customer on a 24/7 basis, and includes the then-current SOC 3 report, ISO 27001 certification and other applicable privacy and security documentation. Customer acknowledges and agrees that the Compliance Resources are provided by AWS, and Eved has no control over, and has no liability for, the accuracy or completeness of the contents thereof.

2.2. **<u>Customer Data</u>.** Eved acknowledges and agrees that, in the course of its engagement by Customer, Eved may create, receive, or have access to Customer Data. Eved shall comply with the terms and conditions set forth in the Agreement and this Exhibit in its creation, collection, receipt, transmission, storage, disposal, use, and disclosure of such Customer Data and be responsible for any unauthorized creation, collection, receipt, transmission, access, storage, disposal, use, or disclosure of Customer Data under its control or in its possession by all Authorized Representatives in breach of the Agreement or this Exhibit.

Eved shall be responsible for, and remain liable to, Customer for the actions and omissions of all Authorized Representatives concerning the treatment of Customer Data as if they were Eved's own actions and omissions.

## 3. INFORMATION SECURITY.

3.1. **Compliance with Laws and Regulations.** Eved represents and warrants that its creation, collection, receipt, access, use, storage, disposal, and disclosure of Customer Data does and will comply with all applicable federal, state, and international privacy and data protection laws, as well as all other applicable regulations and directives, including, to the extent applicable, the EU General Data Protection Regulation 2016/679.

3.2. **Written Information Security Policy.** Eved shall implement and maintain a written information security program including appropriate policies, procedures, and risk assessments that are reviewed at least annually.

3.3. **Safeguards.** Without limiting Eved's obligations under Section 3.1, Eved shall implement commercially reasonable administrative, physical, and technical safeguards to protect Customer Data from unauthorized access, acquisition, or disclosure, destruction, alteration, accidental loss, misuse, or damage that are no less rigorous than generally accepted industry practices and shall otherwise ensure that all such safeguards, including the manner in which Customer Data is created, collected, accessed, received, used, stored, processed, disposed of, and disclosed, comply with applicable data protection and privacy laws, as well as the terms and conditions of the Agreement and this Exhibit.

3.4. **Minimum Safeguards.** At a minimum, Eved's safeguards for the protection of Customer Data shall include: (a) limiting access of Customer Data to Authorized Representatives; (b) securing business facilities, data centers, paper files, servers, backup systems, and computing equipment, including, but not limited to, all mobile devices and other equipment with information storage capability; (c) implementing network, application, database, and platform security; (d) securing information transmission, storage, and disposal; (e) implementing authentication and access controls within media, applications, operating systems, and equipment; (f) encrypting Customer Data stored on any mobile media; (g) encrypting Customer Data transmitted over public or wireless networks; (h) conducting risk assessments, penetration testing, and vulnerability scans and promptly implementing, at Eved's sole cost and expense, a corrective action plan to correct any issues that are reported as a result of the testing; (i) implementing appropriate personnel security and integrity procedures and practices, including, but not limited to, conducting background checks for its employees consistent with applicable law; and (j) providing appropriate privacy and information security training to Eved's employees.

3.5. **Compliance by Authorized Representatives.** Eved shall require each Authorized Representative to be subject to a written obligation to comply with Eved's written information security program and shall maintain a disciplinary process to address any failure to so comply.

## 4. SECURITY INCIDENT PROCEDURES.

4.1. **Incident Response Plan.** Eved maintains a cyber incident breach response plan in accordance with generally accepted industry standards and will implement the procedures required under such plan on the occurrence of a Security Incident.

4.2. **Security Contacts.** Eved shall: (a) provide Customer with the name and contact information of Eved which shall serve as Customer's primary security contact and shall be available to assist Customer via telephone on Business Days during the hours of 4:00 AM and 5:00 PM Central Time and all other times via email as a contact in resolving obligations associated with a Security Incident; and (b) notify Customer via telephone or email of a Security Incident as soon as practicable, but no later than seventy-two (72) hours after Eved becomes aware of it.

4.3. **Notification of Security Incidents.** Immediately following Eved's notification to Customer of a Security Incident, the Parties shall coordinate with each other to investigate the Security Incident. Eved agrees to reasonably cooperate with Customer in Customer's handling of the matter, including, without limitation: (a) assisting with any investigation; and (b) making available all relevant records, logs, files, data reporting, and other materials required to comply with applicable law, regulation, industry standards, or as otherwise reasonably required by Customer.

4.4. **Security Incident Containment.** Eved shall at its own expense take reasonable steps to immediately contain and remedy any Security Incident and prevent any further Security Incident, including, but not limited to taking any and all action necessary to comply with applicable privacy rights, laws, regulations, and standards.

4.5. **Notice to Affected Individuals.** Eved agrees that it shall not inform any third-party of any Security Incident without first obtaining Customer's prior written consent, other than to inform a complainant that the matter has been forwarded to Customer's legal counsel. Further, Eved agrees that Customer shall have the sole right to determine: (a) whether notice of the Security Incident is to be provided to any individuals, regulators, law enforcement agencies, consumer reporting agencies, or others as required by law or regulation, or otherwise in Customer's discretion; and (b) the contents of such notice, whether any type of remediation may be offered to affected persons, and the nature and extent of any such remediation. Notwithstanding the foregoing, nothing in this Section 4.5 shall prohibit Eved from making a general statement, or a statement related to any other customer of Eved's data, to any individuals, regulators, law enforcement agencies, consumer reporting agencies, or others.

4.6. **Record Maintenance.** Eved agrees to maintain and preserve all documents, records, and other data related to any Security Incident.

4.7. **Cooperation.** Eved agrees to reasonably cooperate with Customer in any litigation, investigation, or other action deemed reasonably necessary by Customer to protect its rights relating to the use, disclosure, protection, and maintenance of Customer Data.

4.8. **Prevention.** In the event of any Security Incident, Eved shall promptly use its reasonable efforts to prevent a recurrence of any such Security Incident.

5. **OVERSIGHT OF SECURITY COMPLIANCE.** Subject to Section 2.1, at least once per year, Eved shall conduct a security controls review and/or audit of the Hosted Services by a recognized third-party audit firm based on recognized industry standards. Eved will promptly address any exceptions noted by such security controls review and/or audit with the development and implementation of a corrective action plan by Eved's management. Eved will make results of such controls review or audit available to Customer upon request and will timely address noted exceptions. Customer shall treat such audit results as Eved's Confidential Information under the Agreement.