DATA PROCESSING ADDENDUM

This Data Processing Addendum ("DPA") is effective as of ______________ between Cvent Canada Inc. ("Cvent") and the customer specified in the table below ("Customer").

<table>
<thead>
<tr>
<th>Cvent Canada, Inc.</th>
<th>Customer: &lt;Legal Name&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature:</td>
<td>Signature:</td>
</tr>
<tr>
<td>Name:</td>
<td>Name:</td>
</tr>
<tr>
<td>Title:</td>
<td>Title:</td>
</tr>
<tr>
<td>Date Signed:</td>
<td>Date Signed:</td>
</tr>
<tr>
<td>Contact Information:</td>
<td>Contact Information:</td>
</tr>
</tbody>
</table>

Cvent and Customer shall hereafter be collectively known as the “Parties” and individually known as a “Party”. To the extent that any of the terms or conditions contained in this DPA may contradict or conflict with any terms or conditions regarding the processing of personal data in any agreements between the Parties (each an “Agreement”, and collectively referred to as the “Agreements”), it is expressly understood and agreed that the terms of this DPA shall take precedence and supersede those other terms or conditions.

The Parties agree as follows:

1. DEFINITIONS

1.1 For the purposes of this DPA, the following expressions bear the following meanings unless the context otherwise requires:

“Applicable Data Protection Laws” means, in respect of a Party, any law, statute, declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule or other binding instrument relating to the protection of personal data, including:

(a) the Directive 2002/58/EC (as amended) (the “e-Privacy Directive”), the e-Privacy Regulation 2017/003 (COD) (the “e-Privacy Regulation”), once it takes effect, and any laws implementing these;

(b) the Directive 95/46/EC (as amended) (the “Data Protection Directive”), the Regulation 2016/679 (the General Data Protection Regulation, “GDPR”), once it takes effect, and any laws implementing these.

(in each case as amended, consolidated, re-enacted or replaced from time to time);

“Data Subject”, “Personal Data”, “Process”, “Processed” or “Processing” shall each have the meaning as set out in the GDPR;

“EU Data Protection Laws” means any law, statute, declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule or other binding instrument relating to the protection of personal data in
force in the territory of the European Union, including the Data Protection Directive, the GDPR, the e-Privacy Directive and the e-Privacy Regulation;

“Model Clauses” mean the Standard Contractual Clauses (Controller to Processor) as set out in the Commission Decision of 5 February 2010 (C (2010) 593);

“Privacy Shield” means the EU-US and Swiss-US Privacy Shield Frameworks as designed by the US Department of Commerce and approved by the European Commission and Swiss Administration (respectively) to as having adequate protection under the Data Protection Directive and the GDPR (once it takes effect) and the Swiss 235.1 Federal Act of 19 June 1992 on Data Protection (respectively);

“Regulator” means the data protection supervisory authority which has jurisdiction over a Data Controller’s Processing of Personal Data; and

“Third Countries” means all countries outside of the scope of the data protection laws of the European Economic Area (“EEA”), excluding countries approved as providing adequate protection for Personal Data by the European Commission from time to time, which at the date of this DPA include Andorra, Argentina, Canada, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay.

2. PROCESSING OF PERSONAL DATA

2.1 The Parties acknowledge and agree that with regard to the Processing of Personal Data, Customer is the “Data Controller”, Cvent is the “Data Processor” and that Cvent will engage “Sub-Processors” pursuant to the requirements set forth in Section 8 below.

2.2 The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule 1 “Processing Details” of this DPA.

2.3 The Data Processor shall only process the Personal Data on behalf of and in accordance with documented instructions from the Data Controller. The parties agree that this DPA is Customer’s complete instructions to Cvent in relation to processing of Customer Data. The Data Controller shall ensure that its instructions comply with all Applicable Data Protection Laws, and that the Processing of Personal Data in accordance with Data Controller’s instructions will not cause Data Processor to be in breach of the Applicable Data Protection Laws. The Data Controller shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which the Data Controller acquired Personal Data.

2.4 Each Party will comply with all laws, rules and regulations applicable to it and binding on it in the performance of this DPA, including Applicable Data Protection Laws.

3. AUTHORIZED PERSONNEL

3.1 The Data Processor shall ensure that its personnel authorized to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. The Data Processor shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

4. RIGHTS OF DATA SUBJECTS

4.1 The Data Processor shall, to the extent legally permitted, promptly notify the Data Controller if it receives a request from a Data Subject for access to its own Personal Data, or for the rectification or erasure of such Personal Data or any other request or query from a Data Subject relating to its own Personal Data (including Data Subjects’ exercising rights under Applicable Data Protection Laws, such as rights of objection, restriction of processing, data portability or the right not to be subject to automated decision making) (a “Data Subject Request”). Taking into account the nature of the Processing, the Data Processor shall assist the Data Controller by appropriate technical and organizational measures, insofar as this is possible, for the
fulfilment of the Data Controller’s obligation to respond to a Data Subject Request under Applicable Data Protection Laws. In addition, to the extent the Data Controller, in its use of the services, does not have the ability to address a Data Subject Request, the Data Processor shall upon Data Controller’s request provide commercially reasonable efforts to assist the Data Controller in responding to such Data Subject Request, to the extent the Data Processor is legally permitted to do so and the response to such Data Subject Request is required under Applicable Data Protection Laws. To the extent legally permitted, the Data Controller shall be responsible for any costs arising from the Data Processor’s provision of such assistance.

5. **GOVERNMENT ACCESS REQUESTS**

5.1 The Data Processor shall promptly notify the Data Controller about any legally binding request for disclosure of Personal Data by a law enforcement authority, unless otherwise prohibited from doing so.

6. **SECURITY**

6.1 The Data Processor shall implement and maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Personal Data), confidentiality and integrity of Personal Data.

7. **COMPLIANCE**

7.1 The Data Processor will, subject to confidentiality arrangements that will satisfy both parties, make available to the Data Controller all information necessary to demonstrate compliance with the obligations laid down in this DPA and Applicable Data Protection Laws.

7.2 Upon Data Controller’s request, the Data Processor shall provide the Data Controller with reasonable cooperation and assistance needed to fulfil Data Controller’s obligation under the GDPR to carry out a data protection impact assessment related to Data Controller’s use of the services, to the extent the Data Controller does not otherwise have access to the relevant information, and to the extent such information is available to the Data Processor. The Data Processor shall provide reasonable assistance to the Data Controller in the cooperation or prior consultation with the Regulator in the performance of its tasks relating to Section 12.1 of this DPA, to the extent required under the GDPR.

8. **SUB-PROCESSING**

8.1 The Data Controller agrees that the Data Processor may engage Sub-Processors to Process Personal Data. The Data Processor shall ensure that such Sub-Processor has entered into a written agreement requiring the Sub-Processor to abide by terms no less protective than those provided in this DPA. Upon Data Controller’s request, the Data Processor will make available to the Data Controller a summary of the data processing terms. The Data Processor shall be liable for the acts and omissions of any Sub-Processors to the same extent as if the acts or omissions were performed by the Data Processor.

8.2 The Data Processor shall make available to the Data Controller a list of Sub-Processors authorized to Process Personal Data (“Sub-Processor List”) and provide the Data Controller with a mechanism to obtain notice of any addition or changes to the Sub-Processors, including a formal mechanism to reasonably object to any intended additions or changes.

8.3 This Section 8.3 shall apply only where and to the extent that the Data Controller is established within the EEA or Switzerland or where otherwise required by Applicable Data Protection Laws. In such event, if the Data Controller objects on reasonable grounds relating to data protection to the Data Processor’s use of a new Sub-Processor then the Data Controller shall promptly, and within fourteen (14) days following Data Processor’s notification pursuant to Section 8.2 above, provide written notice of such objection to the Data Processor. Should the Data Processor choose to retain the objected-to Sub-Processor, the Data Processor will notify the Data Controller at least fourteen (14) days before authorizing the Sub-Processor to Process Personal
Data and the Data Controller may immediately discontinue using the services and may terminate the relevant Agreement within thirty (30) days.

9. **RETURN AND DELETION**

9.1 The Data Processor shall, at the request of the Data Controller, delete or return all the Personal Data to the Data Controller after the end of the provision of services relating to Processing, and delete existing copies of the Personal Data unless prohibited by law or the order of a governmental or regulatory body or it could subject the Data Processor to liability.

10. **DATA BREACH**

10.1 In the event Data Processor becomes aware of any improper, unauthorized or unlawful access to, use of, or disclosure of, or any other compromise which affects the availability, integrity or confidentiality of Personal Data which is Processed by Data Processor under or in connection with this DPA and/or the Agreement (“Data Breach”), Data Processor shall:

10.1.1 without undue delay notify Data Controller in writing of all known details of the Data Breach relating to the Personal Data, including:

   a) a description of the nature of the Data Breach including, where possible, the categories and approximate number of Data Subjects and records concerned;

   b) the name and contact details of the data protection officer or other contact point where more information can be obtained;

   c) a description of the likely consequences of the Data Breach; and

   d) a description of the measures taken or proposed to be taken to address the Data Breach, including, where appropriate, measures to mitigate its possible adverse effects;

10.1.2 mitigate any harmful effect that is known to Data Processor of a use or disclosure of the Personal Data in violation of the Agreement or in connection with a Data Breach;

10.1.3 assist Data Controller in remediating or mitigating any potential damage from a Data Breach. Data Processor shall further provide Data Controller with regular status updates on any Data Breach including, but not limited to, actions taken to resolve such incident, at mutually agreed intervals or times for the duration of the Data Breach;

10.1.4 within 4 weeks of closure of the incident, provide the Data Controller a written report describing the Data Breach, the root cause analysis, actions taken by Data Processor during its response and Data Processor’s plans for future actions to prevent a similar Data Breach from occurring;

10.1.5 unless prohibited by applicable law or a legally-binding request of law enforcement, not disclose to third parties (including Regulators) any information about a Data Breach involving the Personal Data without prior written and express permission from Data Controller for such disclosure; and

10.1.6 provide reasonable assistance to the Data Controller with notifying the Data Breach to any Regulator or the Data Subject in accordance with the Applicable Data Protection Laws.

11. **INTERNATIONAL TRANSFERS**

11.1 In the event that Data Controller transfers Customer Personal Data to the Data Processor and the Data Processor makes routine transfers of Customer Personal Data in the normal course of business to its Affiliates and these transfers include any Customer Personal Data that the Applicable Data Protection Laws apply to,
such transfers, if to the United States, will be made pursuant to the EU-U.S. and Swiss-U.S. Privacy Shield Program. Transfers that are made to third countries without a Commission adequacy decision other than the United States will be made subject to appropriate safeguards provided for by the Model Clauses.

11.2 If the Data Processor Affiliate in the United States is not Privacy Shield certified, or in case the Privacy Shield certification ceases to be considered to provide adequate protection to enable the export of personal data in accordance with EU Data Protection Laws, the Data Processor will only process data in, or transfer Personal Data to, a Third Country where such processing or transfer takes place based and in compliance with the Model Clauses, with the processing details that comprise Appendix 1 to the EU Standard Contractual Clauses, and the technical and organizational security measures that comprise Appendix 2 to the Model Clauses. The Data Processor shall comply with the obligations of the data importer and Data Controller shall comply with the obligations of the data exporter as set out in the Model Clauses.

11.3 Where the Data Processor appoints an affiliate or third-party Sub-Contractor to process Personal Data in a Third Country, the Data Processor must ensure that such processing takes place in accordance with the requirements of the Applicable Data Protection Laws (including Privacy Shield principles). The parties agree that Personal Data may be transferred to an affiliate or third-party Sub-Contractor in the United States that is certified to process such data under the Privacy Shield or that agrees to comply with the Privacy Shield principles.

12. GENERAL PROVISIONS

12.1 The Parties hereby acknowledge and agree that a person with rights under this DPA may be irreparably harmed by any breach of its terms and that damages alone may not be an adequate remedy. Accordingly, a person bringing a claim under this DPA shall be entitled to the remedies of injunction, specific performance or other equitable relief for any threatened or actual breach of the terms of this DPA.

12.2 If one of the Party seeks changes to the DPA to comply with a change in Applicable Data Protection Laws or binding and final decision of a Regulator with jurisdiction over the Party’s Processing of Personal Data, the Parties will discuss in good faith how to address any necessary changes.

12.3 The section headings contained in this DPA are for reference purposes only and shall not in any way affect the meaning or interpretation of this DPA.
ATTACHMENT 1

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

Name of the data exporting organisation:

Address:

Tel.: ; fax: ; e-mail:

Other information needed to identify the organisation:

…………………………………………………………………………………………………………………………………………………………………………………………

(the data exporter)

And

Name of the data importing organisation: Cvent Canada, Inc.

Address: 1177 West Hastings Street, Vancouver, BC V6E 2K3

Tel.; fax:Click or tap here to enter text.; e-mail:Click or tap here to enter text.

Other information needed to identify the organisation: Not applicable

(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;
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;

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;

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;

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

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

Clause 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 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 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 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.

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 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. 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.
On behalf of the data importer:

Name (written out in full): Click or tap here to enter text.

Position: Click or tap here to enter text.

Address: Click or tap here to enter text.

Other information necessary in order for the contract to be binding (if any): Click or tap here to enter text.

Signature……………………………………….
(stamp of organisation)

On behalf of the data exporter:

Name Lawrence J. Samuelson

Position: General Counsel & Corporate Secretary

Address: 1765 Greensboro Station Place, Suite 700, Tysons Corner, VA 22102

Other information necessary in order for the contract to be binding (if any):

Signature
(stamp of organisation)
SCHEDULE 1: PROCESSING DETAILS

Processing Activities

The Personal Data Processed by Data Processor will be subject to the following basic Processing activities:

Building and Hosting Event Apps.

Duration

The Personal Data Processed by Data Processor will be Processed for the following duration:

Cvent will retain active customer’s personal data only as long as necessary. Data will only be disposed of upon customer request. Inactive customer data may be retained for a minimum of two years, or until customer’s consent for earlier disposal.

Data Subjects

The Personal Data Processed by Data Processor concern the following categories of Data Subjects:

Event Participants (which includes, but not limited to, attendees, speakers, and authors.)

Categories of Data

The Personal Data Processed by Data Processor includes the following categories of data:

Category:

- Personally Identifiable Information (PII): PII is any information pertaining to an individual that can be used to distinguish or trace a person’s identity.
- Social Data: Photos, Comments and likes
- User Activity Data

Please Note: Clients are discouraged from storing protected/sensitive PII, PCI (Payment Card Industry) or HIPPA (Health Insurance Portability and Accountability Act) related data using Cvent’s systems and applications, and do so at their own risk.
Protected/Sensitive PII is Personally Identifiable Information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.

Protected/Sensitive PII include:

- Social security numbers
- Bank account numbers
- Passport information
- Healthcare related information
- Medical insurance information
- Student information
- Credit and debit card numbers
- Drivers license and State ID information
Special Categories of Data (if appropriate)

The Personal Data Processed by Data Processor concern the following special categories of data:

None