AMENDMENT
TO
GDPR DATA PROTECTION ADDENDUM

This Amendment ("Amendment") to the [GDPR DATA PROTECTION ADDENDUM] entered into by and between [CUSTOMER] located at _____ ("Customer"), and Cvent, Inc., a Delaware corporation located at 1765 Greensboro Station Place, Suite 700, Tysons Corner, Virginia 22102, on behalf of itself and its wholly-owned subsidiaries (collectively, "Cvent") as of [DATE] (the "DPA"), is hereby made and entered into effective as of July 16, 2020 (the "Amendment Effective Date").

WHEREAS, Cvent and Customer are parties to that certain DPA;

WHEREAS, the basis for transfer of personal data to Cvent (if to the United States) were previously made pursuant to the EU-U.S. Privacy Shield or the Standard Contractual Clauses adopted by the European Commission;

WHEREAS, the Court of Justice of the European Union ruled on July 16, 2020 the EU-U.S. Privacy Shield was an invalid mechanism for international transfer of personal data and confirmed that international data flows under EU Data Protection Laws can continue to be based on the standard data protection clauses adopted by the Commission ("Standard Contractual Clauses");

WHEREAS, new contractual clauses were adopted by the Commission Implementing Decision (EU) 2021/679 as of 4 June 2021 for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("2021 Standard Contractual Clauses").

WHEREAS, the parties desire to amend the DPA, effective as of the Amendment Effective Date, consistent with the terms and conditions of this Amendment.

NOW, THEREFORE, in consideration of the mutual covenants contained herein, the parties hereby agree as follows:

1. Definitions. Capitalized terms used in this Amendment shall have the meaning ascribed to them in the DPA unless otherwise specifically defined herein. The Whereas clauses set forth above are hereby incorporated into and made a part of this Amendment as if fully set forth herein.

2. Amended Terms and Conditions. The parties agree to amend the DPA as follows:

a. Notwithstanding anything set forth in the DPA, the Parties hereby agree to the following:

"Cvent makes available the follow transfer mechanism which shall apply, in the same order of precedence as set out below, to any transfers of Customer Personal Data under this DPA from the European Union, the European Economic Area and/or their member states, and Switzerland to countries which do not ensure an adequate level of data protection within the meaning of European Data Protection Laws of the foregoing territories, to the extent such transfers are subject to such European Data Protection Laws: 2021 Standard Contractual Clauses, attached hereto as Attachment 1. Data transfers from the United Kingdom to a restricted country hereunder shall apply the Standard Contractual Clauses as previously executed by the parties."

b. Add Appendix 1 of this Amendment as "Attachment 2" to the DPA.

c. For the purposes of the 2021 Standard Contractual Clauses:

i. Customer shall be deemed the "data exporter" and Cvent the "data importer."

ii. The Parties agree to apply Module Two of the Standard Contractual Clauses, reflecting transfer from controller to processor.

iii. The Parties elect not to include Clause 7 of the Standard Contractual Clauses (Optional Docking Clause).

iv. With respect to Clause 11, the Parties agree not to provide the right to lodge a complaint with an independent dispute resolution body (as is optional under Clause 11(a), "Redress").

v. With respect to Clause 9, the Parties select the "Option 2 General Written Authorisation" under Module Two.

vi. With respect to Clause 13 and Annex I.C, the competent supervisory authority is _____.

vii. With respect to Clause 17 of the Standard Contractual Clauses, the Parties select, under Option 1, the law of _____.

viii. With respect to Clause 18 of the Standard Contractual Clauses, the Parties agree that any dispute arising from the Standard Contractual Clauses shall be resolved by the courts of _____.

3. General Provisions. Except as expressly amended by this Amendment, the terms and conditions set forth in the DPA shall remain in full force and effect. In the event of any conflict between the DPA and this Amendment, the terms and conditions of this Amendment shall govern.

4 Counterparts. This Amendment may be executed in any number of counterparts, each of which when so executed will be deemed an original, and all of which together, shall constitute one and the same agreement. Signatures sent by facsimile or similar means (including scanned images of signatures forwarded by e-mail) shall have the same binding effect as original signatures.

IN WITNESS WHEREOF, the Parties hereto have executed this Amendment on the date specified below.

CVENT, INC.	**[CUSTOMER]**
Signature: _____	Signature: _____
Printed Name: _____	Printed Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

Appendix 1:

Attachment 2:

COMMISSION IMPLEMENTNG DECISION (EU) 2021/914 of 4 June 2021 on

STANDARD CONTRACTUAL CLAUSES

for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council

ANNEX

SECTION I

Clause 1

Purpose and scope

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

(b) The Parties:

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

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

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

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

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

Clause 2

Effect and invariability of the Clauses

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

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

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
(ii) Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);
(iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);
(iv) Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);
(v) Clause 13;
(vi) Clause 15.1(c), (d) and (e);
(vii) Clause 16(e);
(viii) Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7 – Optional

Docking clause

[Intentionally Omitted]

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

MODULE TWO: Transfer controller to processor

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

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

8.3 Transparency

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

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

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

8.6 Security of processing

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

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

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

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

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union ([4]) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

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

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

(a) OPTION 1: Not Selected

OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least [*Specify time period*] in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. ([8]) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

MODULE TWO: Transfer controller to processor

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

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

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

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

[OPTION: Not Selected]

MODULE TWO: Transfer controller to processor

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

MODULE TWO: Transfer controller to processor

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a

processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

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

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

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

Clause 13

Supervision

MODULE TWO: Transfer controller to processor

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

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

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

Clause 14

Local laws and practices affecting compliance with the Clauses

MODULE TWO: Transfer controller to processor

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

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

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

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ([12]);

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

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

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

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

MODULE TWO: Transfer controller to processor

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

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

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

15.2 Review of legality and data minimisation

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

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

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

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

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

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

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

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

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

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

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

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

Clause 17

Governing law

MODULE TWO: Transfer controller to processor

[OPTION 1: These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of _____ (*specify Member State*).]

[OPTION 2 (for Modules Two and Three): These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of _____ (*specify Member State*).]

Clause 18

Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of _____ (*specify Member State*).

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

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

([2]) This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible.

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

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

([5]) See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article 29(4) of Regulation (EU) 2018/1725.

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

([7]) This includes whether the transfer and further processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences.

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

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

([10]) That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.

([11]) The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

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

APPENDIX

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or

contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

MODULE TWO: Transfer controller to processor

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

1. Name: …

   Address: …

   Contact person's name, position and contact details: …

   Activities relevant to the data transferred under these Clauses: …

   Signature and date: …

   Role (controller/processor): controller

2. N/A …

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

1. Name: Cvent, Inc, on behalf of itself and its wholly-owned Affiliates.

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

   Contact person's name, position and contact details: Lawrence Samuelson, Senior Vice President, General Counsel, and Corporate Secretary

   Activities relevant to the data transferred under these Clauses:

   Signature and date: …

   Role (controller/processor): processor

2. N/A …

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

Categories of data subjects whose personal data is transferred
Customer's clients (attendees, submitters, survey respondents, customer's employees and associates, RFP submitters, Customer's business contacts, current and prospective customers, members, marketing partners, or other third party contacts that use Services to interact with Customer etc.).

Categories of personal data transferred

- Basic and contact data: name, organization, title, postal address, e-mail address, telephone number, fax number, social media account ID, also credit or debit card number, or other payment account number, as well as applicable expiration dates and billing or shipping addresses;

- Usage data: browser and device information, operating system, device type, system and performance information, app usage data, information collected through cookies, pixel tags and other technologies, general geographic location;

- Further data about a person: dietary preferences, interests, activities, age, gender, education and occupation.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

No special categories of data are processed.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

The frequency of the transfer of Personal Data is determined by Customer. Personal Data is transferred each time that Customer instructs Cvent to process Personal Data.

Nature of the processing

The nature of the processing of Personal Data pertains to the provision of Services under the Agreement.

Purpose(s) of the data transfer and further processing

The purpose of the processing of Personal Data pertains to the provision of Services under the Agreement.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

The retention period of Personal Data is generally determined by Customer and is subject to the term of the DPA and the Agreement.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Subject Matter, nature and duration of processing by sub-processors will never be beyond the scope of what is conducted by data importer.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer controller to processor

Identify the competent supervisory authority/ies in accordance with Clause 13

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE TWO: Transfer controller to processor

Description of the technical and organisational security measures implemented by Cvent

In its provision of services, Cvent may have access to confidential information of Customer and to personally identifiable information of Customer's event registrants, survey respondents and others (collectively, "Customer Data"). Cvent has implemented administrative, technical, and physical safeguards and other reasonable measures that are appropriate to protect Customer Data against unauthorized disclosure, loss and misuse ("Information Security Measures") as provided below, and Cvent will continue to perform these or equivalent measures subject to the terms and conditions of the Agreement:

1. **Information Security Program**. Cvent shall maintain an Information Security program based on generally accepted industry Information Security standards and frameworks (e.g., the then current version of ISO/IEC 27001 or NIST Cybersecurity Framework). Cvent shall also maintain PCI-DSS compliance for all Cvent services and/or systems which process, transmit and/or store credit card information. The Information Security program shall be in place to plan, implement, manage and monitor processes to meet Cvent information security objectives and requirements applicable to Cvent Services. The Information Security program shall also include performing Information Security Risk Assessments. The Information Security Risk Assessments will be performed on an annual basis with a purpose of identifying, ranking and resolving security risks through treatment activities according to a documented, risk-based methodology. Results of internal Information Security Risk Assessments are deemed Confidential to Cvent and are not available for external review or use.

2. **Information Security Policy**. Cvent shall maintain a policy that identifies Information Security Program goals and sets forth Information Security control objectives. The policy shall outline critical roles and responsibilities for Information Security across Cvent's business operations and govern maintenance of relevant implementation standards, guidelines and/or procedures. It shall also be reviewed annually and communicated to employees and applicable third parties. Cvent's Information Security Policy and its associated Information Security Procedures can be shared with customers upon request (and Cvent shall support one request per customer organization on an annual basis).

3. **Information Security Awareness and Employee Training**. Cvent shall maintain an Information Security Awareness Program geared to its employees and relevant third parties to provide understanding for Cvent's Information Security Program, common threats and risks to Customer Data resources, as well as fulfillment of their Information Security responsibilities. As part of the Security Awareness Program, Security Awareness training shall be conducted on an annual basis to all employees and contractors of Cvent; topics covered may include, but are not limited to, Security Policy & Incident Recording, Acceptable Use, Information Classification and Privacy, specifically, concerning GDPR and CCPA.

4. **Personnel Security**. Cvent shall further provide for the security of Customer Data by requiring all Cvent employees undergo identity and criminal background checks upon hire, as permitted by applicable law. Cvent employees shall agree to adopting appropriate measures and requirements upon on-boarding to maintain the confidentiality and non-disclosure of Customer Data. All employees may be subject to disciplinary actions if in violation of Cvent's security policies and/or customer obligations, as mandated through Cvent's policies. All

employees are required to sign a Non-Disclosure Agreement and Acceptable Use Policy which outlines the acceptable use of Cvent assets and Customer Data handling.

5. **Physical Security.** Cvent information hosting and processing facilities shall maintain secure areas and physical entry controls to provide for prevention of unauthorized physical access or exposure, damage, loss, and/or theft of Customer Data. Hosting facilities shall be equipped with 24/7 camera monitoring with logs retained for forensics. Entry to the facilities shall have layered security controls, including badged access for authorized individuals and strict visitor policies. Equipment housing Customer Data within facilities as well as mobile computing devices shall be reasonably safeguarded against unauthorized physical access, damage, loss or theft, as well as environmental threats that may disrupt processing of Customer Data. Hosting facilities shall have safeguards against fire hazards and electricity outages with such safeguards maintained and tested regularly. Storage media containing Customer Data shall be encrypted and be securely overwritten prior to its disposal or re-use. Customer Data will be accessed outside the USA by Cvent's designated employees using strict data security and access controls, for the sole purpose of supporting the necessary activities required for the agreed upon services.

6. **Access Control**. Cvent shall maintain reasonable access controls to authorize, limit and monitor Cvent employee and Cvent contractor access to Customer Data maintained in Cvent's information systems. Controls shall include: multi-factor authentication over a secured VPN connection to any systems hosting Production Data; processes to provision user access with formally approved authorization using unique authentication IDs per individual; managing and reviewing privileged user access rights on a quarterly basis and performing a full review on an annual basis; and prompt removal of user access upon termination of employee or contractor status with Cvent. User passwords and other login information used to facilitate user identification and access to Cvent information systems shall be protected from unauthorized access by secure login mechanisms. Passwords shall be required to be changed every ninety (90) days and accounts shall be disabled after a specific number of invalid login attempts. Role-Based Access Controls shall be in place to ensure that only authorized Employees have access to any systems that could store or transmit Customer Data.

7. **Customer Data Protection**. Cvent shall maintain reasonable controls to safeguard Customer Data maintained in Cvent systems from unauthorized access, exposure, modification, and/or loss. Controls to protect Customer Data may include, but are not limited to, the following: Protecting Customer Data in transit and while at rest, as required by Cvent's Information Classification standard, by implementing strong cryptography controls using AES-256 for specifically handling PII and Customer financial data. All backups containing Customer Data shall be encrypted and all databases logically separated to ensure the confidentiality of Customer Data. Procedures shall be in place for maintaining encrypted backups of Customer Data in a secure area(s) and securely disposing or destroying Customer Data using techniques consistent with NIST 800-88, "Guidelines for Media Sanitization" or other similar industry standards.

8. **Network and System Security**. Cvent shall maintain reasonable controls to operate Information Systems that maintain Customer Data. Controls include, but are not limited to: logical and/or physical network segmentation for Development and/or Production regions, network segregation between DMZs and systems hosting sensitive data, controlling and monitoring network access, network filtering devices, firewalls, intrusion detection systems, anti-virus & anti-malware solutions, and logging capabilities to detect and respond to unauthorized or suspicious activity. Cvent shall actively monitor for known security events and anomalies that may pose a threat to Customer Data. Additionally, Cvent shall also maintain a Change Management process to control significant planned and unplanned changes to Cvent's Information Systems.

9. **Vulnerability Management**. Cvent shall maintain processes to identify, evaluate and address vulnerabilities that may be present on Cvent Information Systems and SaaS applications. Cvent shall perform annual penetration

testing and quarterly vulnerability scanning on all publicly-addressable systems as well as internal production and corporate systems. PCI ASV scans shall be conducted for all publicly addressable systems within PCI scope and work with an industry accredited third party to perform penetration testing on all Cvent PCI-scoped systems. Customers shall be provided with an Executive Summary report of our external scan report upon written request. Cvent uses the Common Vulnerability Scoring System (CVSS) 3.1 and internal risk assessment methodologies to prioritize vulnerabilities and address within reasonable timeframes to reduce the risk of potential exploitation that may lead to system compromise, loss of system availability, or unauthorized access to system(s) or Customer Data. Defined risk levels and corresponding timeframes in accordance with the aforementioned standards are as follows: Critical (Prioritized over other work until fixed, in no case later than 7 days), High (30 days), Medium (90 days) and Low (at the discretion of Cvent). Cvent shall assess different risk levels and remediation timelines in its sole discretion, based upon business impact of the remediation and the underlying risk of the vulnerability. Any vulnerabilities that cannot be resolved are subject to a formal Risk Acceptance with appropriate documented justification, with relevant compensating controls in place and formal approval from C-Level Management.

10. **Secure Software Development**. Cvent shall maintain processes to identify, evaluate and address risks to the development of its software solutions. Cvent shall maintain an independent test/development environment, separate from production computing resources, for any testing of new software and/or changes to existing software. Production data will not be used for software testing and development purposes unless sanitized and deemed necessary for any intended testing that needs to be performed; all efforts will be made to first utilize mock/test data. Cvent maintains a change control process for application changes pushed to production computing environments. Changes shall require approvals and specific tasks to be performed, including: Development, Code Review, Testing, Approval of Changes, and Documentation of Changes. Cvent requires all software developers to undergo training on secure coding practices in line with OWASP Top 10 guidelines.

11. **Third Party/Supply Chain Security**. Cvent shall maintain a process to identify, evaluate and manage risks associated with third-party vendors and/or service providers. Third parties that access, process, or store Customer Data shall undergo Risk Assessment. Reassessments of critical third parties shall be performed on an annual basis. Risks identified through risk assessments shall be prioritized and documented by Cvent.

12. **Security Incident Management.** Cvent shall maintain processes to identify, respond to, contain and minimize the impact of Information Security incidents to Customer Data. A "Security Incident" shall be defined as an event that results in the unauthorized disclosure of any personally identifiable or confidential Customer Data. In the event of a Security Incident of Customer Data while maintained in Cvent systems, Cvent shall notify Customer no later than forty-eight (48) hours after the Breach has been confirmed. The notice shall include the approximate date and time of the Breach and a summary of relevant, then-known facts, including a description of measures being taken to further investigate and address the Breach.

13. **Business Continuity Management**. Cvent shall maintain controls to recover Information Systems hosting Customer Data to reasonably acceptable levels in the event of an unplanned disruption whose root cause is attributed to an entity or force beyond Cvent's reasonable ability to control. Controls shall include a Business Continuity or Disaster Recovery Plan, which includes, but may not be limited to addressing backup(s) of Customer Data; a process to test such backup(s) at regular intervals; providing a description of resources and steps required to recover Information Systems to acceptable levels of performance and performing testing of the Business Continuity or Disaster Recovery Plan(s) on an annual basis.

14. **Compliance and Audits.** Cvent shall hire a qualified external audit firm to conduct an audit of Cvent's product offerings and its supporting infrastructure and processes on an annual basis. The audits shall result in a valid certificate/report for an industry acceptable framework such as SOC1, SOC2, PCI DSS, ISO 27001 and others as

needed. Upon written request, Cvent shall share any relevant audit certificates or its SOC reports with its customers when requested in writing by the customer.

ANNEX III

LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor

EXPLANATORY NOTE:

This Annex must be completed for Modules Two and Three, in case of the specific authorisation of sub-processors (Clause 9(a), Option 1).

The controller has authorised the use of the following sub-processors:

https://www.cvent.com/uk/gdpr/cvents-affiliates-and-subprocessors