Socio Labs, LLC
115 W Washington Street Ste 1190
Indianapolis, IN. 46204
+1-877-336-2888

DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") forms part of the Terms of Service available at https://socio.events/termsofservice ("**Terms**") or any other written or electronic agreement for the purchase of the Socio Service as identified in such agreement (collectively "**Principal Agreement**") between Socio; and the entity listed in the signature block below ("**Customer**"). Socio and Customer are each a "Party" and collectively, the "Parties".

Except as modified below, the Principal Agreement shall remain in full force and effect.

In consideration of the mutual obligations set out herein, the Parties hereby agree that:

The terms and conditions set out below shall be added as an addendum to the Principal Agreement.

Except where the context requires otherwise, references in this DPA to the Principal Agreement are to the Principal Agreement as amended by, and including, this DPA.

DEFINITIONS AND INTERPRETATION

In this DPA, the following terms shall have the meanings set out below and cognate Principal Agreement shall be construed accordingly:

"Applicable Data Privacy Law" means EU General Data Protection Regulation 2016/679 ("GDPR"), California Consumer Privacy Act of 2018 ("CCPA") or any other applicable data protection or privacy law where applicable;

"Approved Jurisdiction" means a member state of the EEA, or other jurisdiction approved as having adequate legal protections for data by the European Commission, currently found here: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

"Customer Personal Data" means any Personal Data or Personal Information Processed by Socio on behalf of the Customer pursuant to or in connection with the Principal Agreement and this DPA;

"Standard Contractual Clauses" means the agreement set forth in Exhibit 2 as approved by the European Commission for the transfer of Personal Data to Processors established in third countries which do not ensure an adequate level of data protection and any subsequent changes approved by the European Commission with an official decision;

Capitalized terms not otherwise defined herein shall have the meaning given to them in the Principal Agreement or the Applicable Data Privacy Law.

The word "**include**" shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

Socio Labs, LLC
115 W Washington Street Ste 1190
Indianapolis, IN. 46204
+1-877-336-2888

1. PROCESSING OF CUSTOMER PERSONAL DATA

1.1. **Role of the Parties.** The Parties acknowledge and agree that with regard to the Processing of Customer Personal Data in Exhibit 1, Customer is the Controller (or Business), Socio is the Processor (or Service Provider), and that Socio will engage Subprocessors pursuant to the requirements set out in Clause 4 Subprocessors below.

1.2. **Customer's Processing of Customer Personal Data.** Customer shall, in its use of the Services and instructions to Socio:

a) comply with Applicable Data Privacy Law in their Processing of Customer Personal Data; and

b) have sole responsibility for the accuracy, quality and legality of Customer Personal Data as provided by Customer to Socio and the means by which Customer acquired Customer Personal Data.

1.3. **Socio's Processing of Customer Personal Data.** Socio shall:

a) comply with Applicable Data Privacy Law in their Processing of Customer Personal Data; and

b) treat Customer Personal Data as Confidential Information; and

c) not Process Customer Personal Data other than on the relevant Customer's documented instructions unless Processing is required by Applicable Data Privacy Law, in which case Socio shall to the extent permitted by applicable laws inform Customer of that legal requirement before the relevant Processing of that Customer Personal Data; and

d) act and shall continue to act, solely as Customer's Processor (or Service Provider) with respect to all Customer Personal Data transferred to Socio under the Principal Agreement; and

e) be prohibited from selling Customer Personal Data, and retaining, using, or disclosing Customer Personal Data outside of the direct business relationship between Customer and Socio.

Socio certifies that Socio understands the restrictions in this clause and will comply with them in accordance with Applicable Data Privacy Laws.

1.4. **Processing Instructions.** Customer instructs Socio and authorises Socio to Process Customer Personal Data; and transfer Customer Personal Data according to clause 10, as reasonably necessary:

a) for the provision of the Services and consistent with the Principal Agreement and this DPA;

b) to comply with other documented reasonable instructions provided by Customer where such instructions are consistent with the Principal Agreement and this DPA.

1.5. **Details of the Processing.** Exhibit 1 to this DPA sets out:

Socio Labs, LLC
115 W Washington Street Ste 1190
Indianapolis, IN. 46204
+1-877-336-2888

a) the subject matter and duration of the Processing of Customer Personal Data;

b) the nature and purpose of the Processing of Customer Personal Data;

c) the categories of Data Subject (or Consumer) to whom the Customer Personal Data relates; and

d) the types of Customer Personal Data to be Processed.

2. DATA SUBJECT (OR CONSUMER) RIGHTS

2.1. **Data Subject (or Consumer) Request.** Socio shall, to the extent legally permitted, notify Customer at the email address associated with the licence owner and/or Event Planner as defined in the Principal agreement without undue delay if Socio receives a request from a Data Subject (or Consumer) to exercise the Data Subject's (or Consumer's) right of access (or disclosure), right to rectification, restriction of Processing, erasure (or deletion or the "right to be forgotten"), data portability, object to the Processing, or its right not to be subject to an automated individual decision making ("**Data Subject (or Consumer) Request**"). The Parties must not discriminate against a Consumer because they exercised their rights.

2.2. **Socio Assistance.** Taking into account the nature of the Processing, Socio shall reasonably assist Customer by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer's obligations to respond to requests to exercise Data Subject (or Consumer) rights under the Applicable Data Privacy Law. Socio shall not be liable for Customer's failure to address Data Subject (or Consumer) Requests.

3. SOCIO PERSONNEL

3.1. **Confidentiality**. Socio shall ensure that its personnel engaged in the Processing of Customer Personal Data are informed of the confidential nature of Customer Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements or are under an appropriate statutory obligation of confidentiality. Socio shall ensure that confidentiality obligations regarding Customer Personal Data survive the termination of the personnel engagement.

3.2. **Limitation of access**. Socio shall ensure in each case that access is strictly limited to those individuals who need to know / access the relevant Customer Personal Data, as strictly necessary for the purposes of the Principal Agreement and this DPA, and to comply with Applicable Data Privacy Laws in the context of that individual's duties to Socio.

4. SUBPROCESSING

4.1. **Appointment**. Customer authorises Socio to appoint Subprocessors in connection with the Services and in accordance with this Clause 4.

Socio Labs, LLC
115 W Washington Street Ste 1190
Indianapolis, IN. 46204
+1-877-336-2888

4.2. **Current Subprocessors**.

SUBPROCESSOR	PURPOSE	PERSONAL DATA	LOCATION WHERE PERSONAL DATA IS PROCESSED
Hubspot	Customer management; Customer success	Planner profile data	USA
Salesforce	Customer management	Planner profile data	USA
Intercom	Attendee support	Attendee profile data, Participant content data, Sponsor profile data	USA
Google	Platform as a Service; database hosting; authentication; push notifications; analytics	Attendee profile data, Participant content data, Planner profile data, Sponsor profile data	USA
Twilio	Transactional email messaging; SMS messaging	Attendee profile data, Planner profile data, Sponsor profile data	USA
Filestack	Web service for file uploads	Attendee profile data, Participant content data, Sponsor profile data	USA
Bugsnag	Web service for error logging	Attendee profile data, Attendee technical data	USA
Amazon / AWS	Platform as a Service; database hosting; event analytics; transactional email messaging; streaming	Attendee profile data, Participant content data, Planner profile data, Attendee technical data	USA
Amplitude	Web service for application analytics	Attendee profile data, Attendee technical data	USA
Segment.io	Web service for analytics data collection and transfer	Attendee technical data	USA

Restream	Captures livestream content	Planner profile data	USA

Our parent company Cisco Systems Inc. and its subsidiaries may also act as Subprocessors in some circumstances under Standard Contractual Clauses entered into.

4.3. **New Subprocessors**. Socio will notify customers of new Subprocessors by updating the list of Subprocessors on the Website. Customer may also sign up to receive notifications of new Subprocessors via e-mail by e-mailing legal@socio.events with the subject "Subscribe to New Sub-processor Notifications" and specifying the email address such notifications should be sent to. If, within a reasonable time specified in the notice, Customer notifies Socio in writing of any objections to the proposed appointment based on reasonable grounds relating to data protection: Socio shall work with Customer in good faith to make available a commercially reasonable change in the provision of the Services which avoids the use of that proposed Subprocessor. Where such a change cannot be made, notwithstanding anything in the Principal Agreement, Customer may by written notice to Socio with immediate effect terminate the relationship to the extent that it relates to the Services which require the use of the proposed Subprocessor. Such termination is without prejudice to any fees incurred by Customer prior to the termination.

4.4. With respect to each Subprocessor, Socio shall:

a) carry out adequate due diligence before the Subprocessor first Processes Customer Personal Data to ensure that the Subprocessor is capable of providing the level of protection for Customer Personal Data required by the Applicable Data Privacy Law;

b) ensure that the arrangement between Socio and the Subprocessor, is governed by a written contract including Principal Agreement which offer at least the same level of protection for Customer Personal Data as those set out in the Applicable Data Privacy Law.

4.5. **Liability**. Socio shall be liable for the acts and omissions of its Subprocessors to the same extent Socio would be liable if performing the services of each Subprocessor directly under the Principal Agreement of this DPA.

4.6. For the purposes of Clause 9 of the Standard Contractual Clauses, Customer provides a general consent to Socio to engage Subprocessors. Such consent is conditional on Socio's compliance with Section 4 of this DPA.

5. SECURITY

5.1. **Socio obligations.** Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and

severity for the rights and freedoms of natural persons, Socio shall, at its cost and expense, in relation to Customer Personal Data implement appropriate technical and organizational measures in accordance with the Security Appendix: Socio Technical and Organisational Measures available at https://socio.events/docs/infosecappx to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in the Applicable Data Privacy Law, especially Article 32 of the GDPR. In assessing the appropriate level of security, Socio shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

5.2. These measures should entail physical, logical and data access control as well as data transfer, instruction, entry, availability and separation control.

5.3. **Customer obligations**. Notwithstanding the above, Customer agrees that except as provided by this DPA, Customer is responsible for its secure use of the Services, including securing its account authentication credentials, protecting the security of Customer Personal Data when in transit to and from the Services.

6. PERSONAL DATA BREACH

6.1. Socio shall notify Customer at the email address associated with the licence owner and/or Event Planner as defined in the Principal Agreement without undue delay upon Socio confirming a Personal Data Breach affecting Customer Personal Data, providing Customer with sufficient information to allow Customer to meet its obligations to report or inform Data Subject (or Consumers) of the Personal Data Breach under the Applicable Data Privacy Law.

6.2. Socio shall co-operate with Customer and take such reasonable commercial steps as are directed by Customer to assist in the investigation, mitigation and remediation of each such Personal Data Breach, as permitted by any involved law enforcement agencies.

6.3. Socio shall promptly resolve as far as possible, at its own cost and expense, all data protection and security issues discovered by Customer and reported to Socio that reveal a breach or potential breach by Socio of its obligations under the Applicable Data Privacy Law.

6.4. If Socio is in breach of its obligations under this DPA, Customer may suspend the transfer of Customer Personal Data to Socio until the breach is remedied.

7. ASSISTANCE, INFORMATION, RECORDS AND AUDIT

7.1. Socio shall reasonably assist the Customer in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR taking into account the nature of processing and the information available.

7.2. Socio shall cooperate with reasonable requests by Customer for legally required security audit (subject to mutual agreement on the time, duration, place, scope and manner of the audit), and respond to reasonable requests for the executive summary of any testing reports once the

Customer enters into a non-disclosure agreement with Socio. Socio shall make available to Customer, upon written request and without undue delay, copies of any third party audit reports or certifications it maintains that apply to the Service, to the extent that Socio maintains such certifications in its normal course of business.

7.3. Customer acknowledges and agrees that any exercise of its audit rights under Clause 8.9 of the Standard Contractual Clauses will be conducted in accordance with this DPA.

8. DELETION OR RETURN OF CUSTOMER PERSONAL DATA

8.1. Socio shall, at the choice of the Customer, delete or return all the Customer Personal Data to the Customer after the end of the provision of Services, and deletes existing copies unless applicable law requires storage of the Customer Personal Data.

9. LIMITATION OF LIABILITY

9.1. Each Party's liability, taken together in the aggregate, arising out of or related to this DPA, whether in contract, tort or under any other theory of liability is subject to the limitation of liability clauses of the Principal Agreement.

10. TRANSFER MECHANISMS

10.1. **Transfers** of Personal Data **from EEA or Switzerland to third countries.** Where Socio Processes Personal Data from the EEA or Switzerland on behalf of Customer, in a country which is not an Approved Jurisdiction, Socio shall perform such Processing in accordance with the Standard Contractual Clauses set forth in Exhibit 2 to this DPA and/or in accordance with Articles 44 to 49 of the GDPR.

10.2. **Transfers of Personal Data from the UK to third countries**. Where Socio Processes Personal Data from the UK in a third country, such Processing shall be performed in accordance with Exhibit 2, as amended by the UK Addendum to the EU Commission Standard Contractual Clauses available at https://ico.org.uk/media/about-the-ico/consultations/2620398/draft-ico-addendum-to-com-scc-20210805.pdf

11. Term

11.1. The term of this DPA shall correspond to the term of the Principal Agreement.

12. Validity and Effective Date

12.1. This DPA is entered into from the date of the last signature and valid and effective from the date the other Party receives the countersigned copy.

12.2. This DPA may be executed electronically. The Parties expressly waive any right to object to the validity, effectiveness or enforceability of an electronically signed DPA. By placing a name or other identifier in connection with this DPA, the Party doing so intends to sign the DPA with the signature attributed to the content. The last Party to which the signed DPA has been

delivered via the respective e-mail address, sends the DPA with electronic signature back to the sending Party. For the avoidance of any doubt, the Parties agree that their signatures can be replaced by mechanical means, i.e. by the electronic signature, unless a qualified electronic signature is used.

12.3. This DPA may be executed (including use of e-signature technology) in one or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument.

13. Authority and Third Parties

13.1. Parties warrant and represent that they have full power and authority to enter into and perform their respective obligations under the DPA.

13.2. Except as otherwise provided hereunder or under applicable law, no one other than a Party to this DPA, its successors and permitted assigns shall have any right to enforce any of its terms.

14. Governing Law and Jurisdiction

14.1. The Parties to this DPA hereby submit to the jurisdiction of Santa Clara County courts with respect to any disputes or claims howsoever arising under this DPA, and this DPA and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of California notwithstanding the conflict of law provisions and other mandatory legal provisions.

15. Order Of Precedence

15.1. The Parties agree that DPA shall replace any existing DPA the Parties may have previously entered into in connection with the Services.

15.2. Nothing in this DPA reduces Socio's obligations under the Principal Agreement in relation to the protection of Customer Personal Data or permits Socio to Process (or permit the Processing of) Customer Personal Data in a manner which is prohibited by the Principal Agreement.

15.3. With regard to the subject matter of this DPA, in the event of inconsistencies between the provisions of this DPA and any other agreements between the parties, including the Principal Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the Parties) agreements entered into or purported to be entered into after the date of this DPA, the provisions of this DPA shall prevail.

16. Severance

16.1. Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended

Socio Labs, LLC
115 W Washington Street Ste 1190
Indianapolis, IN. 46204
+1-877-336-2888

as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

IN WITNESS WHEREOF, this DPA is entered into and becomes a binding part of the Principal Agreement.

For and on behalf of Customer:

Signature _____

Name _____

Title _____

Date Signed _____

For or on behalf of Socio, Socio Labs, LLC
115 W. Washington Street
Suite 1190
Indianapolis, Indiana 46204:

Signature _____

Name _____

Title _____

Date Signed _____

Socio Labs, LLC
115 W Washington Street Ste 1190
Indianapolis, IN. 46204
+1-877-336-2888

EXHIBIT 1: DETAILS OF PROCESSING OF CUSTOMER PERSONAL DATA

This Exhibit 1 includes certain details of the Processing of Customer Personal Data as required by Applicable Data Privacy Law.

Subject matter and duration of the Processing of Customer Personal Data

***Subject matter*:** The subject matter of the Processing under this DPA is the types of Customer Personal Data as listed in this Exhibit 1.

***Duration*:** Personal Data may be Processed and stored for the period necessary to fulfil the agreed purposes of processing pursuant to and for the duration of this DPA and to comply with Applicable Data Privacy Law. This will generally be for the Term plus the period from the expiry of the Term until deletion of all Customer Data by Socio in accordance with its back up policies.

The Service offers certain controls for the Users to delete their data. Requests for users to delete their data, as permitted by law, can be requested via email to privacy@socio.events.

The nature and purpose of the Processing of Customer Personal Data

***Nature*:** Socio provides a software as a service event platform solution through a cloud based platform that enables real-time planning, active engagement of participants at Events organised by Event Planners as described in the Principal Agreement.

***Purpose*:** The purpose of the Customer Personal Data Processing under this DPA is:

a) to allow Socio to provide the Services to the Customer as described in the Principal Agreement and consistently with this DPA;

b) to comply with other documented reasonable instructions provided by Customer where such instructions are consistent with the Principal Agreement and this DPA or to process requests initiated by Customer or Customer's Users in their use of the Services;

c) to comply with any legal obligation.

The categories of Data Subject (or Consumer) to whom the Customer Personal Data relates

Attendees and/or participants of Customer's Events

The types of Customer Personal Data to be Processed under this DPA

Any Customer Personal Data submitted by attendees and/or participants via the Service in their sole discretion contained in:

- Attendee Profile Data (name, email address(es), password, photograph, event enrolments)
- Attendee Technical Data (device information, location, application usage)

Socio Labs, LLC
115 W Washington Street Ste 1190
Indianapolis, IN. 46204
+1-877-336-2888

- Participant Content Data (presentation material, chat, video, in-app interactions)
- Planner Profile Data (name, email address(es), password, photograph)
- Planner Purchase Data (invoice contents, in-app credits purchased)
- Sponsor Profile Data (name, email address, password, photograph, company)

Special categories of data

It is against the Principal Agreement to submit special categories of data via the Service.

Socio Labs, LLC
115 W Washington Street Ste 1190
Indianapolis, IN. 46204
+1-877-336-2888

[Exhibit 2 applies *in case of the conditions in Section 10 of the DPA and/or GDPR requirements are applicable to the Agreement*]

EXHIBIT 2: STANDARD CONTRACTUAL CLAUSES

Standard Contractual Clauses (controller to processor)

COMMISSION IMPLEMENTING 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

(Text with EEA relevance)

For purposes of this Exhibit 2: any reference to "data exporter" means Customer, acting as data exporter on behalf of its EEA or Swiss customer(s) where applicable, and any reference to "data importer" means Socio each a "**party**"; together "**the parties**".

The parties have agreed on the following Standard 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 Annex I.

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.

Socio Labs, LLC
115 W Washington Street Ste 1190
Indianapolis, IN. 46204
+1-877-336-2888

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
Docking clause

a. An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

b. Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

c. The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

Socio Labs, LLC
115 W Washington Street Ste 1190
Indianapolis, IN. 46204
+1-877-336-2888

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 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.

Socio Labs, LLC
115 W Washington Street Ste 1190
Indianapolis, IN. 46204
+1-877-336-2888

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 (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:

a. 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;

b. 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;

c. 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

d. 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. 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 14 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

b. Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. 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.

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

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

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

Clause 14
Local laws and practices affecting compliance with the Clauses

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;

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.

Socio Labs, LLC
115 W Washington Street Ste 1190
Indianapolis, IN. 46204
+1-877-336-2888

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 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.] 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

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 the Netherlands.

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 the Netherlands.

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.

Socio Labs, LLC
115 W Washington Street Ste 1190
Indianapolis, IN. 46204
+1-877-336-2888

Annex I To Exhibit 2

The Standard Contractual Clauses

This Annex I forms part of the Clauses.

A. List of Parties

Data exporter

The data exporter is Customer, acting as data exporter on behalf of itself or a customer where applicable. Activities relevant to the transfer include the performance of services for Customer and its customer(s).

Role: Controller

Data importer

The data importer is Socio. Activities relevant to the transfer include the performance of services for Customer and its customer(s).

Role: Processor

B. Description of transfer

1. Categories of data subjects whose personal data is transferred

Attendees and/or participants of Customer's Events

2. Categories of personal data transferred

The personal data transferred may concern the following categories of data:

Any Customer Personal Data submitted by attendees and/or participants via the Service in their sole discretion contained in:

- Attendee Profile Data (name, email address(es), password, photograph, event enrolments)
- Attendee Technical Data (device information, location, application usage)
- Participant Content Data (presentation material, chat, video, in-app interactions)
- Planner Profile Data (name, email address(es), password, photograph)
- Planner Purchase Data (invoice contents, in-app credits purchased)
- Sponsor Profile Data (name, email address, password, photograph, company)

3. 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.

It is against the Principal Agreement to submit special categories of data via the Service.

Socio Labs, LLC
115 W Washington Street Ste 1190
Indianapolis, IN. 46204
+1-877-336-2888

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

The Transfer happens on a continuous basis.

5. **Nature of Processing**

Socio provides a software as a service event platform solution through a cloud based platform that enables real-time planning, active engagement of participants at Events organised by Event Planners as described in the Principal Agreement.**Purpose(s) of the data transfer and further processing**

The purpose of the Customer Personal Data Processing under this DPA is:

a) to allow Socio to provide the Services to the Customer as described in the Principal Agreement and consistently with this DPA;

b) to comply with other documented reasonable instructions provided by Customer where such instructions are consistent with the Principal Agreement and this DPA or to process requests initiated by Customer or Customer's Users in their use of the Services;

c) to comply with any legal obligation.

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

Personal Data may be Processed and stored for the period necessary to fulfil the agreed purposes of processing pursuant to and for the duration of this DPA and to comply with Applicable Data Privacy Law. This will generally be for the Term plus the period from the expiry of the Term until deletion of all Customer Data by Socio in accordance with its back up policies.

The Service offers certain controls for the Users to delete their data. Requests for users to delete their data, as permitted by law, can be requested via email to privacy@socio.events.

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

Personal data will be transferred to Socio's sub-processors as set forth in Section 4.2. of the DPA.

C. **COMPETENT SUPERVISORY AUTHORITY**

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

The data exporter's competent supervisory authority will be determined in accordance with the GDPR.

The Standard Contractual Clauses

Annex II to Exhibit 2, the Standard Contractual Clauses, is the Security Appendix: Socio Technical and Organisational Measures available at https://socio.events/docs/infosecappx.

Socio Labs, LLC
115 W Washington Street Ste 1190
Indianapolis, IN. 46204
+1-877-336-2888

Annex III To Exhibit 2

List of Sub-processors

Personal data will be transferred to Socio's sub-processors as set forth in Section 4.2. of the DPA.