The Client agreeing to this Boomset Data Processing Addendum (the DPA or "Addendum") and Boomset, Inc. ("Boomset") have executed the online version of the Boomset Master Service Agreement (the "Service Agreement"), of which this Addendum forms a part.

The terms used in this Addendum shall have the meanings set forth in this Addendum. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Principal Agreement. Except as modified below, the terms of 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 Addendum to the Principal Agreement are to the Principal Agreement as amended by, and including, this Addendum.

1. Definitions

1.1 In this Addendum, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

1.1.1 "**Applicable Laws**" means (a) European Union or Member State laws with respect to any Company Personal Data in respect of which the Company is subject to EU Data Protection Laws; and (b) any other applicable law with respect to any Company Personal Data in respect of which Company is subject to any other Data Protection Laws;

1.1.2 "**Company Personal Data**" means any Personal Data Processed by Processor on behalf of Company pursuant to or in connection with the Principal Agreement;

1.1.3 "**Data Protection Laws**" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

1.1.4 "**EEA**" means the European Economic Area;

1.1.5 "**EU Data Protection Laws**" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;

1.1.6 "**GDPR**" means EU General Data Protection Regulation 2016/679;

1.1.7 "**Restricted Transfer**" means:

1.1.7.1 an onward transfer of Company Personal Data from a Subprocessor by Vendor.

in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws) in the absence of the Standard Contractual Clauses to be established under section 12 below;

1.1.8 "**Services**" means the services and other activities to be supplied to or carried out by or on behalf of Vendor for Company pursuant to the Principal Agreement;

1.1.9 "**Standard Contractual Clauses**" means the contractual clauses set out in Annex 2, amended as indicated (in square brackets and italics) in that Annex and under section 13.4;

1.1.10 "**Subprocessor**" means any person (including any third party, but excluding an employee of Vendor or any of its sub-contractors) appointed by or on behalf of Vendor to Process Personal Data on behalf of Company in connection with the Principal Agreement; and

1.2 The terms, "**Commission**", "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

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

2. Processing of Company Personal Data

2.1 Vendor shall:

2.1.1 comply with all applicable Data Protection Laws in the Processing of Company Personal Data; and

2.1.2 not Process Company Personal Data other than on the relevant documented instructions from Company unless Processing is required by Applicable Laws to which Vendor is subject, in which case Vendor shall to the extent permitted by Applicable Laws inform the Company of that legal requirement before the relevant Processing of that Personal Data.

2.2 Company shall:

2.2.1 instruct Vendor (and authorises Vendor to instruct each Subprocessor) to:

2.2.1.1 Process Company Personal Data; and

2.2.1.2 in particular, transfer Company Personal Data to any country or territory,

as reasonably necessary for the provision of the Services and consistent with the Principal Agreement; and

2.2.2 warrants and represents that it is and will at all relevant times remain duly and effectively authorised to give the instruction set out in section 2.2.1.

2.3 Annex 1 to this Addendum sets out certain information regarding the Subprocessors' Processing of the Company Personal Data as required by article 28(3) of the GDPR (and, possibly, equivalent requirements of other Data Protection Laws). Company may make reasonable amendments to Annex 1 by written notice to Vendor strictly to the extent necessary to meet those requirements. Nothing in Annex 1 (including as amended pursuant to this section 3.3) confers any right or imposes any obligation on any party to this Addendum.

3. Vendor Personnel

Vendor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Subprocessor who may have access to the Company Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Company Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Subprocessor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. Security

4.1 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, Vendor shall, in relation to the Company Personal Data, as instructed by Company, implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

4.2 In assessing the appropriate level of security, the parties shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

5. **Subprocessing**

5.1 Company authorises Vendor to appoint Subprocessors in accordance with this section 5 and any restrictions in the Principal Agreement.

5.2 Vendor may continue to use those Subprocessors already engaged by Vendor as at the date of this Addendum, subject to Vendor in each case as soon as practicable meeting the obligations set out in section 5.4.

5.3 Vendor shall give Company prior written notice of the appointment of any new Subprocessor, including full details of the Processing to be undertaken by the Subprocessor. If, within five (5) business days of receipt of that notice, Company notifies Vendor in writing of any objections (on reasonable grounds) to the proposed appointment:

5.3.1 Vendor shall not appoint (or disclose any Company Personal Data to) that proposed Subprocessor until reasonable steps have been taken to address the objections raised by any Company has been provided with a reasonable written explanation of the steps taken.

5.4 With respect to each Subprocessor, Vendor shall:

5.4.1 before the Subprocessor first Processes Company Personal Data (or, where relevant, in accordance with section 5.2), carry out adequate due diligence to ensure that the Subprocessor is capable of providing the level of protection for Company Personal Data required by the Principal Agreement;

5.4.2 ensure that the arrangement between Vendor and the relevant Subprocessor is governed by a written contract including terms which offer at least the same level of protection for Company Personal Data as those set out in this Addendum and meet the requirements of article 28(3) of the GDPR;

5.4.3 if that arrangement involves a Restricted Transfer, ensure that the Standard Contractual Clauses are at all relevant times incorporated into the agreement between Vendor and the Subprocessor, or before the Subprocessor first Processes

Company Personal Data, procure that it enters into an agreement incorporating the Standard Contractual Clauses with Company; and

5.4.4 provide to Company confirmation of the existence of Vendor's agreements with Subprocessors as Company may request from time to time.

5.5 Vendor shall ensure that each Subprocessor performs the obligations under sections 2.1, 3, 4, 6.1 , 7.2, 8 and 10.1, as they apply to Processing of Company Personal Data carried out by that Subprocessor, as if it were party to this Addendum in place of Vendor.

6. Data Subject Rights

6.1 Taking into account the nature of the Processing, Vendor shall assist Company by implementing appropriate technical and organizational measures, insofar as this is possible and reasonable, for the fulfilment of the Company's obligations, as reasonably understood and communicated by Company to Vendor, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

6.2 Vendor shall:

6.2.1 promptly notify Company if any Subpocessor receives a request from a Data Subject under any Data Protection Law in respect of Company Personal Data; and

6.2.2 ensure that the Subprocessor does not respond to that request except on the documented instructions of Company or as required by Applicable Laws to which the Subprocessor is subject, in which case Vendor shall to the extent permitted by Applicable Laws inform Company of that legal requirement before the Subprocessor responds to the request.

7. **Personal Data Breach**

7.1 Vendor shall notify Company promptly upon Vendor or any Subprocessor becoming aware of a Personal Data Breach affecting Company Personal Data, providing Company with sufficient information to allow it to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

7.2 Vendor shall co-operate with Company and take such reasonable commercial steps as are directed by Company to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. Data Protection Impact Assessment and Prior Consultation

Vendor shall provide reasonable assistance to Company with any data protection impact assessments, and prior consultations with Supervising Authorities having jurisdiction over Company, which Company reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Company Personal Data by, and taking into account the nature of the Processing and information available to Vendor.

9. Deletion or return of Company Personal Data

9.1 Subject to sections 9.2 and 9.3 Vendor shall promptly after the date of cessation of any Services involving the Processing of Company Personal Data (the "**Cessation Date**"), delete all copies of those Company Personal Data.

9.2 Subject to section 9.3, Company may in its absolute discretion by written notice to Vendor require Vendor to (a) return a complete copy of all Company Personal Data to Company by secure file transfer in such format as is reasonably notified by Company to Vendor; and (b) delete and procure the deletion of all other copies of Company Personal Data Processed by any Subprocessor. Vendor's compliance with such request shall be at Company's expense.

9.3 Each Subprocessor may retain Company Personal Data to the extent required by Applicable Laws and only to the extent and for such period as required by Applicable Laws and always provided that Vendor shall ensure the confidentiality of all such Company Personal Data and shall ensure that such Company Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage and for no other purpose.

9.4 Vendor shall provide written certification to Company that it has fully complied with this section 9.

10. Audit rights

10.1 Subject to sections 10.2 to 10.3, Vendor shall make available to Company upon reasonable request all information necessary to demonstrate compliance with this Addendum, and shall allow for and contribute to audits, including inspections, by Company or an auditor mandated or in relation to the Processing of the Company Personal Data by Vendor.

10.2 Information and audit rights of Company only arise under section 10.1 to the extent that the Principal Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law (including, where applicable, article 28(3)(h) of the GDPR).

10.3 Company undertaking an audit shall give Vendor reasonable notice (in no event less than fourteen (14) days) of any audit or inspection to be conducted under section 10.1 and shall make (and ensure that each of its mandated auditors makes) reasonable endeavors to avoid causing (or, if it cannot avoid, to minimize) any damage, injury or disruption to the Vendor's premises, equipment, personnel, data and business while its personnel are on those premises in the course of such an audit or inspection. Vendor need not give access to its premises for the purposes of such an audit or inspection:

10.3.1 to any individual unless he or she produces reasonable evidence of identity and authority;

10.3.2 outside normal business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis and Company has given notice to Vendor that this is the case before attendance outside those hours begins; or

10.3.3 for the purposes of more than one audit or inspection in any calendar year, except for any additional audits or inspections which:

10.3.3.1 Company undertaking an audit reasonably considers necessary because of genuine concerns as to Vendor's compliance with this Addendum; or

10.3.3.2 Company is required or requested to carry out by Data Protection Law, a Supervisory Authority or any similar regulatory authority responsible for the enforcement of Data Protection Laws in any country or territory,

11. General Terms

Governing law and jurisdiction

11.1 Without prejudice to clauses 7 (Mediation and Jurisdiction) and 9 (Governing Law) of the Standard Contractual Clauses:

11.1.1 the parties to this Addendum hereby submit to the choice of jurisdiction stipulated in the Principal Agreement with respect to any disputes or claims howsoever arising under this Addendum, including disputes regarding its existence, validity or termination or the consequences of its nullity; and

11.1.2 this Addendum and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Principal Agreement.

Order of precedence

11.2 Nothing in this Addendum reduces Vendor's obligations under the Principal Agreement in relation to the protection of Personal Data or permits Vendor to Process (or permit the Processing of) Personal Data in a manner which is prohibited by the Principal Agreement. In the event of any conflict or inconsistency between this Addendum and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

11.3 Subject to section 12.2, with regard to the subject matter of this Addendum, in the event of inconsistencies between the provisions of this Addendum 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 Addendum, the provisions of this Addendum shall prevail.

Changes in Data Protection Laws, etc.

11.4 Company may:

11.4.1 by at least 30 (thirty) calendar days' written notice to Vendor from time to time make any variations to the Standard Contractual Clauses (including any Standard Contractual Clauses entered into under section 11.1), as they apply to Restricted Transfers which are subject to a particular Data Protection Law, which are required, as a result of any change in, or decision of a competent authority under, that Data Protection Law, to allow those Restricted Transfers to be made (or continue to be made) without breach of that Data Protection Law; and

11.4.2 propose for mutual agreement in writing any other variations to this Addendum which Company reasonably considers to be necessary to address the requirements of any Data Protection Law.

11.5 If Company gives notice under section 12.4.1:

11.5.1 Company shall not unreasonably withhold or delay agreement to any consequential variations to this Addendum proposed by Vendor to protect the Subprocessor against additional risks associated with the variations made under section 12.4.1.

11.6 If Company gives notice under section 12.4.2, the parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified in Company's notice as soon as is reasonably practicable.

Severance

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

SCHEDULE 1: List of Approved Sub-Processors
As of Execution Date of DPA

Pursuant to Art. 5.b of the Addendum, below is a list of Boomset's current Subprocessors as of the Effective Date:

Subprocessor Name	Location of Processing
Amazon Web Services, Inc.	United States of America
Base CRM	United States of America
LogMeIn	United States of America
New Relic	United States of America
Postmark	United States of America
Readme	United States of America
Sentry	United States of America
Slack	United States of America
Spreedly	United States of America
Stripe	United States of America
Twilio	United States of America
Zapier	United States of America
Zendesk	United States of America

ANNEX 1: DETAILS OF PROCESSING OF COMPANY PERSONAL DATA

This Annex 1 includes certain details of the Processing of Company Personal Data as required by Article 28(3) GDPR.

Subject matter and duration of the Processing of Customer Personal Data

The subject matter of the Processing of Client Personal Data pertains to the provision of Services, as requested by the Client. Customers gather attendee information which is then exported to the Boomset Guest List in order to facilitate guest registration at the Customer's event.

The duration of the Processing of Client Personal Data is generally determined by the Client and is subject to the term of this Addendum and the Service Agreement, respectively, in the context of the contractual relationship between Boomset and the Client. If the Customer deletes the Attendee Guest list following the conclusion of the event, then the Customer Personal Data is removed from the Boomset systems.

The nature and purpose of the Processing of Customer Personal Data

Boomset does not use event attendee personal information in any way other than as required to allow the Customer to use the Boomset Platform and Services to facilitate event attendee check-in. We do not share attendee personal information with third parties and our Boomset Platform and Services allow Customers to delete attendee data following their event.

The types of Customer Personal Data to be Processed

The types of Customer Personal Data to be processed is specified by the Customer in the Service Agreement.

The categories of Data Subject to whom the Customer Personal Data relates

The categories of Data Subject to whom the Customer Personal Data relates are specified by the Customer as per the Service Agreement.

The obligations and rights of Customer.

The rights and obligations of the Client are set out in the Service Agreement and this Addendum.

ANNEX 2: STANDARD CONTRACTUAL CLAUSES

These Clauses are deemed to be amended from time to time, to the extent that they relate to a Restricted Transfer which is subject to the Data Protection Laws of a given country or territory, to reflect (to the extent possible without material uncertainty as to the result) any change (including any replacement) made in accordance with those Data Protection Laws (i) by the Commission to or of the equivalent contractual clauses approved by the Commission under EU Directive 95/46/EC or the GDPR (in the case of the Data Protection Laws of the European Union or a Member State); or (ii) by an equivalent competent authority to or of any equivalent contractual clauses approved by it or by another competent authority under another Data Protection Law (otherwise).

If these Clauses are not governed by the law of a Member State, the terms "Member State" and "State" are replaced, throughout, by the word "jurisdiction".

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection the Client and Boomset HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Background

The data exporter has entered into a data processing addendum ("DPA") with the data importer. Pursuant to the terms of the DPA, it is contemplated that services provided by the data importer will involve the transfer of personal data to data importer. Data importer is located in a country not ensuring an adequate level of data protection. To ensure compliance with Directive 95/46/EC and applicable data protection law, the controller agrees to the provision of such Services, including the processing of personal data incidental thereto, subject to the data importer's execution of, and compliance with, the terms of these Clauses.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; [*If these Clauses are governed by a law which extends the protection of data protection laws to corporate persons, the words "except that, if these Clauses govern a transfer of data relating to identified or identifiable corporate (as well as natural) persons, the definition of "personal data" is expanded to include those data" are added.*]

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC; [*If these Clauses are not governed by the law of a Member State, the words "and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC" are deleted.*]

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

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

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor

entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

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

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

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

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

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

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

be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC; [*If these Clauses are not governed by the law of a Member State, the words "within the meaning of Directive 95/46/EC" are deleted.*]

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

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

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

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

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

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

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

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

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

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

(ii) any accidental or unauthorised access, and

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

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

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

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

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

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

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

Clause 6

Liability

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

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

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

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

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

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

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be

updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

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

Data exporter
The data exporter is:
Client

Data importer
The data importer is:
Boomset, Inc.

Data subjects
The personal data transferred concern the following categories of data subjects:
Client determines the personal data that is to be transferred.

Categories of data
The personal data transferred concern the following categories of data:
Client determines the categories of personal data. Boomset requires only first and last name of attendees.

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data:
Client determines any special categories requested from attendees.

Processing operations
The personal data transferred will be subject to the following basic processing activities:

Boomset does not use Client's attendee information in any way other than to allow the event organizer to check in the attendee to their event using our software platform.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

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

Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

Data importer has implemented and will maintain the technical and organizational security measures to ensure a level of security appropriate to the risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

Application Security

Our product is designed with security in mind. We make sure security is a core component at every stage of the development lifecycle. Right from the initial planning stage, new features and projects are assessed in terms of their impact on privacy and security. At the design stage, low-level security issues are addressed and approved by the CEO. During development, our programmers abide by programming best practices. Finally, before every release, our QA team carries out security testing and vulnerability scanning.

Boomset currently does not independently maintain, host or transmit customer data. Such data resides with Amazon Web Services ("AWS") secure cloud services platform. All AWS Services are GDPR ready. AWS continually maintains a high bar for security and compliance across all of their global operations. Their industry-leading security provides the foundation for their long list of internationally recognized certifications and accreditations, demonstrating compliance with rigorous international standards, such as ISO 27017 for cloud security, ISO 27018 for cloud privacy, SOC 1, SOC 2 and SOC 3, PCI DSS Level 1 and others. AWS also helps customers meet local security standards such as BSI's Common Cloud Computing Controls Catalogue (C5), which is important in Germany. AWS also complies with the CISPE Data Protection Code of Conduct for Data Protection in the Cloud.

We are careful with any data we collect, whether it is protected by GDPR or otherwise. We only collect and keep what we have to and then only for as long as our customers need the data. Our cautious practices are reflected in our commitments to the privacy and security of the data that you entrust to us.

Data Security

Protecting the confidentiality, integrity and availability of data processed through our services is a fundamental objective of the Boomset security program. We employ strong technical safeguards to ensure that data is protected and the risk of exposure is minimized.

All data and backups are encrypted at rest using Realm.io which uses strong cyphers (AES 256) and securely managed encryption keys to ensure that in the unlikely event that data is compromised, it still cannot be deciphered.

Boomset is an "HTTPS only" application. All data in transit is encrypted using TLS 1.0 and higher (depending on the client browser). In cases where HTTP is used, visitors are automatically redirected to a secure connection. These safeguards ensure that customer data is always encrypted in transit.

Organizational Security

Security controls are only as strong as the people who implement them. We are committed to employing competent individuals who possess the skills required to successfully implement the company's security objectives. We have strong policies and recruitment processes in place, and we continuously strive to improve through internal audits and process enhancements.

Our employees undergo a rigorous screening process to ensure they are suitable individuals to provide our service and to access customer data. Background checks are performed prior to hiring, and every new employee is required to sign confidentiality and information security policies upon joining the organization. All employees are required to undergo mandatory Security and Privacy training on an ongoing basis. Access to data is approved by a manager on a case-by-case basis, and in case of employment termination, we execute policies that revoke access quickly and effectively.