Amplitude Data Processing Addendum

This Data Processing Addendum with EU Standard Contractual Clauses ("**Addendum**") is effective as of the date last signed below ("**Effective Date**") and is by and between Amplitude, Inc. ("**Amplitude**" or "**Processor**") and the customer identified below ("**Customer**"). This Addendum supplements the Order Form and Master Service Agreement or other agreement executed by the parties, which governs Customer's use of the Amplitude Services (collectively, "**Agreement**").

1. Definitions.

"**Amplitude Services**" means the services chosen by Customer as specified in the Agreement.

"**Customer Data**" means all data, including, but not limited to, Customer's end users' events data provided to Amplitude by, or on behalf of, Customer through Customer's use of the Amplitude Services.

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

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means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR.

"**End User**" means an individual that uses Customer's mobile application or website, and that individual's information is transferred at the direction of Customer to Amplitude Services for processing.

"**GDPR**" means Regulation 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, and repealing Directive 95/46/EC (General Data Protection Regulation).

"**Personal Data**" means any information relating to an identified or identifiable natural person (as defined in the GDPR) that Customer or its End Users provide to Amplitude as part of the Amplitude Services.

"**Process**" or "**Processing**" means any operation or set of operations which is performed by Amplitude as part of the Amplitude Services on Personal Data or on sets of Personal Data, whether or not by automated means.

"**Processor**" and "**Controller**" shall have the meanings given in the GDPR.

"**Standard Contractual Clauses**" means the agreement executed by and between Customer and Amplitude and attached to this Addendum as Annex 1 pursuant to European Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council.

Capitalized terms used but not defined in this Addendum will have the meanings provided in the Agreement.

2. Processing of Personal Data*.*

2.1 This Addendum applies when Personal Data is Processed by Amplitude on behalf of

Customer whose End Users are located in the EEA or Switzerland or where Customer is established in the EEA or Switzerland. The control of Customer Personal Data remains with Customer, and as between Customer and Amplitude, Customer will at all times act as the "Controller". Amplitude will act as the "Processor" with respect to Personal Data.

2.2 The subject matter of the Processing under this Addendum is the Personal Data. The duration of the Processing under this Addendum is for the term of the Agreement. The purpose of the Processing of Personal Data under this Addendum is in order for Amplitude to provide the Amplitude Services to Customer. The nature of the Processing is storage of Personal Data and the Amplitude Services more specifically described in the Agreement. The type of data is the data collected by Customer, in its sole discretion, through Customer's use of the Amplitude Services. The data subjects are Customer's End Users accessing and using Customer's mobile application(s), website(s), IoT or other application(s).

2.3 Amplitude will only Process Personal Data in accordance with the provisions of this Addendum and Customer's instructions. Any instructions provided by Customer to Amplitude with respect to the Processing of Personal Data shall comply with all applicable Data Protection Laws relating to privacy and data protection. Customer further agrees that any instructions it provides to Amplitude with respect to the processing of Personal Data shall not cause Amplitude to be in breach of any applicable Data Protection Laws. Amplitude shall not process the Personal Data for purpose other than to provide the Amplitude Services. Amplitude will Process Personal Data in accordance with the EU Data Protection Laws requirements directly applicable to Amplitude's provision of the Amplitude Services.

2.4 Customer must comply with all EU Data Protection Laws related to its use of the Amplitude Services, including, but not limited to, if applicable, registering with the relevant data protection authority in a Member State. Customer is responsible for compliance with its obligation as data controller under EU Data Protection Laws. Specifically, Customer is responsible for providing any required notices and obtaining any required consents from its End Users related to the transfer and Processing of Personal Data and for Customer's decisions and actions concerning the Processing and use of Personal Data under the terms of the Agreement and this Addendum.

3. International transfers of Personal Data. Personal Data that Amplitude processes on Customer's behalf will be transferred to, and stored and processed in, the United States. Customer hereby consents to the transfer of the Personal Data to the United States and Customer consents to the storage and processing of the Personal Data in the United States by Amplitude in order for Amplitude to provide the Amplitude Services. If Customer is transferring Personal Data from the European Economic Area or Switzerland, then the EU Standard Contractual Clauses (which are attached hereto as Annex 1) will apply to that Personal Data. The Standard Contractual Clauses will not apply to Personal Data that is not transferred outside the European Economic Area or Switzerland.

4. Third Party Requests and Confidentiality.

4.1 Amplitude will not disclose Personal Data to any individual or to a third party other than: (i) at the request of Customer; (ii) as provided in this Addendum; (iii) as necessary to provide the Amplitude Services; or (iv) as required by applicable law or a valid and binding order of a law enforcement agency. Except as otherwise required by law, Amplitude will promptly notify Customer of any subpoena, judicial, administrative or arbitral order of an executive or administrative agency or other governmental authority ("**Demand**") that it receives and which relates to the Personal Data. At Customer's request, Amplitude will provide Customer with reasonable information in its possession that may be responsive to the Demand and any assistance reasonably required for Customer to respond to the Demand in a timely manner. Customer acknowledges that Amplitude has no responsibility to interact directly with the entity making the Demand.

4.2 Amplitude will ensure that all employees or those who have the authority to access or Process the Personal Data are bound by obligations of confidentiality with respect to Personal Data. Amplitude will ensure that its employees or those who have the authority to process Personal Data do not process it except on the instructions of Customer. Amplitude will ensure all employees have undertaken training in the laws relating to the handling of Personal Data; and are aware both of Amplitude's duties and their personal duties and obligations under such laws and this Addendum.

5. Personal Data Access. Amplitude will promptly notify Customer if Amplitude receives a request from an End User to exercise the End User's rights under the GDPR, (including right of access, rectification, objection, erasure, data portability, restriction of Processing, or right not to be subject to an automated individual decision making). Amplitude shall provide all reasonable and timely assistance to Customer, including appropriate technical and organizational measures, insofar as this is possible, to enable Customer to respond to any such request from an End User. In the event that any request from a Data Subject is made directly to Amplitude, Amplitude shall promptly inform Customer and provide the full details of the request to Customer.

6. Security. Amplitude has implemented and will maintain appropriate technical and organizational measures, internal controls, and information security routines to ensure a level of security appropriate to the risk of the accidental loss, destruction, alteration, unauthorized disclosure or access, or the unlawful destruction of Personal Data.

7. Security Incident Notification. In the event of any unlawful access to any Personal Data resulting in loss, disclosure, or alteration of Personal Data (each a "Security Incident"), Amplitude will notify Customer without undue delay from when Amplitude becomes aware of the Security Incident. In addition, Amplitude will investigate the Security Incident and provide Customer with detailed information about the Security Incident in order for Customer to comply with any data breach notification requirements under the GDPR. Amplitude will also take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident. Amplitude's obligation to report or respond to a Security Incident as provided herein is not and will not be construed as an acknowledgement by Amplitude of any fault or liability with respect to the Security Incident.

8. Audit and Records.

8.1 Amplitude undergoes annual audits against known, established industry standards, performed by external auditors. Upon Customer's written request, Amplitude will provide Customer with its annual SOC2 Type 2 audit report, ISO 27001 certification, and any other information necessary to demonstrate Amplitude's compliance with its obligations under the terms of this Addendum.

8.2 The parties agree that any audit conducted under this Addendum, including under Clauses 5(f) or 12(2) of the EU Standard Contractual Clauses, shall be conducted in accordance with the specifications identified in this Section 8.2. Customer may not conduct an audit more than once per calendar year unless Customer is required or requested to conduct an audit by a Supervisory Authority or any similar regulatory authority responsible for the enforcement of Data Protection Laws in any country or territory. Customer may contact Amplitude in accordance with the "Notice" provision of the Agreement to request an on-site audit of Amplitude's procedures related to the protection of Customer's Personal Data. Before Customer can conduct an onsite audit of Amplitude's procedures, Amplitude and Customer shall mutually agree upon the timing, scope and duration of the audit. Customer shall reimburse Amplitude for any costs and expenses incurred by Amplitude as a result of the audit. In addition, the audit shall be conducted in such a way to avoid causing (or, if it cannot be avoided, to minimize) any damage, injury or disruption to Amplitude's premises, equipment, personnel and business while Customer's personnel are on those premises in the course of such an audit or inspection. Any audit conducted under this Section 8.2 shall be limited to Amplitude's premises. If the EU Standard Contractual Clauses apply, then nothing herein shall be construed as affecting any supervisory authority's or data subject's rights under the EU Standard Contractual Clauses.

8.3 Amplitude will keep a record of any Processing of Personal Data it carries out on behalf of Customer, which it shall make available to the relevant supervisory authority on request and which shall include:

a. the name and contact details of Amplitude and of Customer on whose behalf it is acting, and where applicable, Customer's representative and the data protection officer;
b. the categories of Processing carried out on behalf of Customer;
c. transfers of Personal Data to a third country or international organization and the basis on which those transfers are compliant; and
d. a description of data security compliance measures taken by Amplitude.

9. Subprocessors. Amplitude shall provide notification to Customer of a new Subprocessor before authorizing any new Subprocessor to Process Personal Data in accordance with the terms of the Agreement. Customer may object to Amplitude's use of a new Subprocessor by notifying Amplitude promptly in writing within thirty (30) days after receipt of Amplitude's notice regarding the new Subprocessor. If Customer objects to the new Subprocessor, Amplitude will use reasonable efforts to make available a change in the Services or Customer's use of the Services to avoid Processing of Personal Data by the Subprocessor objected to by Customer. If Amplitude is unable to make available such change within thirty (30) days of the receipt of the notice from Customer, then Customer may terminate those Services which cannot be provided without the use of the objected to Subprocessor. If Customer terminates the Services, Amplitude will refund Customer any prepaid fees covering the remainder of the term specified in the applicable ordering document following the effective date of termination. Notwithstanding anything provided herein, Customer acknowledges and agrees, that Amplitude may use the subprocessors identified on Annex 2 ("**Subprocessors**") to provide the Amplitude Services. Amplitude shall impose the same data protection obligations as set forth in this Addendum on any Subprocessor prior to the Subprocessor Processing Personal Data. Amplitude remains responsible for its Subprocessors and liable for their acts and omissions as for its own acts and omissions and any references to Amplitude's obligations, acts and omissions in this Addendum shall be construed as referring also to Amplitude's Subprocessors. The parties agree that any audit rights provided under the terms of this Addendum do not extend to Amplitude's Subprocessors' facilities.

10. Data Protection Impact Assessment and Prior Consultation. Upon Customer's request, Amplitude shall provide reasonable assistance to Customer with any data protection impact assessments, and prior consultations with supervisory authorities, which Customer reasonably considers to be required of Customer by Article 35 or 36 of the GDPR, in each case solely in relation to Processing of Personal Data by and taking into account the nature of the Processing and information available to, Amplitude.

11. Termination.

11.1 This Addendum shall continue in full force until the expiration or termination of the Agreement.

11.2 Upon the expiration or termination of the Agreement, Customer may extract Personal Data from the Amplitude Services. Within thirty (30) days from the expiration or termination of the Agreement, Amplitude will delete Personal Data in accordance with the terms of the Agreement, except as may be required by law.

12. Miscellaneous. Customer will treat the terms and conditions of this Addendum as confidential and shall not disclose them to any third party except for Customer's auditors or consultants that need access to this information for the purpose of this business relationship as articulated in this Addendum and the Agreement. The liability of each party under this Addendum

shall be subject to the exclusions and limitations of liability set forth in the Agreement. If there is a conflict between any provision in this Addendum and any provision in the Agreement, this Addendum shall control. Except for changes made by this Addendum, the Agreement remains unchanged and in full force and effect. This Addendum shall not restrict any applicable data protection laws, rules or regulations. If any provision in this Addendum is ineffective or void, this shall not affect the remaining provisions. The parties shall replace the ineffective or void provision with a lawful provision that reflects the business purpose of the ineffective or void provision. In case a necessary provision is missing, the parties shall add an appropriate one in good faith. In case of conflict, the order of precedence in respect of the Processing of Personal Data shall be: this Addendum and then the Agreement. If the EU Standard Contractual Clauses are an integral part of this Addendum, then the EU Standard Contractual Clauses shall prevail. This Addendum supersedes and replaces all previous written and oral agreements, communications and other understandings relating to the subject matter of this Addendum. This Addendum may be executed in one or more counterparts, each of which will be deemed an original and all of which taken together will be deemed to constitute one and the same document.

IN WITNESS WHEREOF, the authorized representatives of both parties have signed this Addendum as of the Effective Date.

Amplitude, Inc.

By: DocuSigned by: Samantha Schmidt 2B8537A707884B5...

Name: Samantha Schmidt

Title: VP of Legal

Date: 2/28/2019

Kerika

By: DocuSigned by: Arun Kumar 20092275B659940E...

Name: Arun Kumar

Title: CEO

Date: 12/13/2019

Annex 1
Standard Contractual Clauses (processors)

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

Name of the data exporting organisation: Kerika

Address: PO Box 514, Issaquah, WA 98027

Tel.: 4252004185 ; fax: Fax ; e-mail: info@kerika.com

Other information needed to identify the organisation:

……
(the data **exporter**)

And
Name of the data importing organisation: Amplitude, Inc.

Address: 631 Howard Street, Floor 5, San Francisco, CA 94105, United States

Tel.: 415-802-9277; e-mail: legal@amplitude.com

Other information needed to identify the organisation:

……
(the data **importer**)
each a “party”; together “the parties”,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection

of individuals with regard to the processing of personal data and on the free movement of such data[1];

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

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

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

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

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

Clause 2

Details of the transfer

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

Clause 3

Third-party beneficiary clause

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

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

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

such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

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

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

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

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

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

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

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

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

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

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

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

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

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

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

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

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

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

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

  (ii) any accidental or unauthorised access, and

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

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

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

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

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

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

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

Clause 6

Liability

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

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

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

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

Clause 7

Mediation and jurisdiction

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

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

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

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

Clause 8

Cooperation with supervisory authorities

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

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same

conditions as would apply to an audit of the data exporter under the applicable data protection law.

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

Clause 9

Governing Law

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

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business 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.

On behalf of the data exporter:
Name (written out in full): Arun Kumar
Position: CEO
Address: P.O. Box 514, Issaquah, WA 98027
Other information necessary in order for the contract to be binding (if any):

DocuSigned by:
Arun Kumar
20092275B65940E...

Signature.....

(stamp of organisation)

On behalf of the data importer: Amplitude, Inc.
Name (written out in full): Samantha Schmidt
Position: VP of Legal
Address: 631 Howard Street, Floor 5, San Francisco, CA 94105, United States
Other information necessary in order for the contract to be binding (if any):

DocuSigned by:
Samantha Schmidt
2B8537A707884B5...

Signature.....

(stamp of organisation)

APPENDIX 1 TO STANDARD CONTRACTUAL CLAUSES

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

Data exporter
The data exporter is (please specify briefly your activities relevant to the transfer):
Data Exporter is the legal entity that has executed the Standard Contractual Clauses as a Data Exporter and any affiliates.

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

Data Importer is Amplitude, Inc., a provider of cloud based product analytics services, which processes personal data upon the instruction of the Data Exporter in accordance with the terms of the Agreement.

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

The personal data transferred by the Data Exporter is determined and controlled by the Data Exporter, in its sole discretion, and includes the personal data of the end-users of Data Exporter's mobile and web applications.

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

The personal data that may be transferred by the Data Exporter is determined and controlled by the Data Exporter, in its sole discretion, and may include the following categories of personal data:

Information about website and application browsing, activity, history, and device information (e.g., device identifiers (not Apple ID), operating system and IP addresses).

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data (please specify):
None.

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

The personal data transferred is processed by the Data Importer to provide the Services pursuant to the Agreement.

DATA EXPORTER
Name: Arun Kumar

Authorised Signature DocuSigned by: Arun Kumar 20092275B65940E...

DATA IMPORTER: Amplitude, Inc.
Name: Samantha Schmidt, VP of Legal

Authorised Signature DocuSigned by: Samantha Schmidt 2B8537A707884B5...

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

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

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

Amplitude abides by the security standards in this Appendix 2. Amplitude may update or modify these security standards from time to time; provided, in all cases, such modifications will not result in a material degradation of the security of the Services during the term of the Agreement.

Amplitude's security controls are designed to address its posture as a cloud-based platform as a service (PaaS) provider. The following concepts apply throughout the Amplitude service delivery environment, and are contextually essential to the understanding of all such security controls:

Data Neutral: The Amplitude PaaS is unaware of which data customers send to it, and will process all data regardless of its nature as long as it fits the pre-defined characteristics that allow it to be processed. Once data is processed by the Amplitude analytics engine, it is stripped of unnecessary information, and made computationally difficult to separate into original event state. Recovering a structured dataset tied to a specific individual is computationally difficult.

No Employee Interaction: Amplitude employees do not directly interact with customer data as part of their normal job duties except for the purpose of providing support services to customers upon the customer's request. Only the Amplitude platform will interact with such data, and only according to the programmatic instructions provided by each Amplitude customer with respect to their data.

Data Immutability: Customer raw data feeds are preserved in their original state, in encrypted form, in customer-specific S3 buckets. Such feeds can be removed at any time upon request.

Shared Responsibility: Amplitude customers are strongly encouraged to not send sensitive data (such as PII, PCI, ePHI, etc.) to the platform, as it is not necessary for the performance of the platform services. Amplitude provides a secure platform, but customers must take care to use it appropriately as well.

Secure Cloud Platform: Amplitude's PaaS is designed according to established industry best security practices, and includes many technical and administrative security controls, such as:

- **Secure data centers**: Amplitude's PaaS is fully embedded within Amazon's AWS, which is a highly secure cloud platform. For more information about Amazon AWS security, refer to https://aws.amazon.com/security/.
- **Security Compliance**: In addition to the numerous compliance standards and certifications in AWS, Amplitude itself undergoes regular audits against known, established industry standards. Amplitude's annual SOC2 report and any other available reports are available to all customers upon request.
- **Security Testing**: Amplitude regularly tests the security of its platform with multiple tools and processes designed to rapidly identify and remediate potential vulnerabilities. Such testing includes vulnerability and code scanning, penetration testing of the network, application and APIs, ethical hacking, and more.
- **Secure Systems, Logging/Monitoring**: Amplitude utilizes system security benchmarks from established sources, such as the Center for Information Security (CIS), for security configuration of its virtual systems in AWS. Amplitude relies on Threatstack from continuous security event collection, correlation, monitoring and alerting within its cloud platform.

- **Security Policy**: Amplitude has developed and implemented security policies that govern all relevant aspects of its security program, and are aligned with SOC2 and ISO27001 requirements. Policies may be made available to customers upon request.
- **Incident Response**: Amplitude's incident response process (IRP) is designed to address all legal, contractual, and regulatory requirements, and ensure that customers are notified as expediently as possible in case an incident impacts them in some way.
- **Known Owner**: Amplitude has designated the Security Leadership Team (SLT), and its members, as the owner of all security activities within the organization.
- **Security Awareness**: Amplitude constantly strives to educate its workforce on issues related to information security, via multiple means and with respect to each employee's job duties.

DATA EXPORTER
Name: Arun Kumar

Authorised Signature DocuSigned by: Arun Kumar 20092275B65940E...

DATA IMPORTER: Amplitude, Inc.
Name: Samantha Schmidt, VP of Legal

Authorised Signature DocuSigned by: Samantha Schmidt 2B8537A707884B5...

Annex 2

List of Authorized Subprocessors

1. Amazon Web Services
2. Snowflake Computing, Inc. (if applicable)