DATA PROCESSING ADDENDUM

The customer identified in the associated Order Form or otherwise subscribing to Services ("**Customer**") and Stream.io, Inc. ("**Stream**") enter into this Data Processing Addendum (including the Exhibits attached hereto, this "**DPA**") as of the DPA Effective Date (as defined below), and this DPA is incorporated into and forms part of that certain Subscription Agreement (as amended, the "**Agreement**") under which Stream will provide certain Services (as described in the Agreement and Order Form, as applicable) to Customer.

This DPA sets forth certain duties and obligations of the parties with respect to the protection, security, processing, and privacy of Personal Data provided or made available to Stream by Customer as part of the Service provided by Stream for Customer under the Agreement. This DPA shall supplement (and not supersede) the Agreement, and shall take precedence solely to the extent of any conflict between this DPA and the Agreement. All capitalized terms used and not expressly defined in this DPA shall have the meanings given to them in the Agreement.

In the course of providing the Services to Customer pursuant to the Agreement, Stream may Process certain Personal Data provided or made available to Stream by Customer on behalf of Customer and the parties agree to comply with the following provisions with respect to any such Personal Data, each acting reasonably and in good faith. The following obligations shall only apply to the extent required by Data Protection Laws and Regulations (as defined below) with regard to the relevant Personal Data (as defined below), if applicable.

1. DEFINITIONS.

1.1 "**CCPA**" means the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act, and any binding regulations promulgated thereunder.

1.2 "**Controller**" means the natural or legal person, public authority, agency, or entity that determines the purposes and means of the Processing of Customer Data.

1.3 "**Customer Data**" is defined in the Agreement as "Customer Data".

1.4 "**Data Protection Laws and Regulations**" means all applicable data privacy and security laws and regulations, including (a) European Data Protection Laws; (b) the CCPA, including any comprehensive United States state privacy laws; and (c) any other data protection law and any guidance or statutory codes of practice issued by any relevant regulatory authority, in each case, as amended from time to time and any successor legislation to the same.

1.5 "**Data Subject**" means the identified or identifiable person to whom Personal Data relates.

1.6 "**DPA Effective Date**" means the date on which the parties agreed to the Agreement.

1.7 "**EEA**" means the European Economic Area.

1.8 "**European Data Protection Laws**" means, to the extent applicable to a party, the EU General Data Protection Regulation 2016/679 ("**EU GDPR**"), any data protection laws relating to data protection, the Processing of Personal Data, privacy or electronic communications in force from time to time in the United Kingdom, including the United Kingdom General Data Protection Regulation, as it forms part of the law of the United Kingdom by virtue of section 3 of the European Union (Withdrawal) Act 2018 and the Data Protection Act 2018, in each case as amended from time to time (including by the Data (Use and Access) Act 2025) ("**UK GDPR**"), the Swiss Federal Act on Data Protection ("**Swiss FDPA**," and together with the EU GDPR and UK GDPR, "**GDPR**"), and any other applicable national rule and legislation on the protection of Personal Data in the European Economic Area that is already in force or that will come into force during the term of this DPA.

1.9 "**Personal Data**" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household contained in Customer Data that is uploaded or submitted to the Services by Customer.

1.10 "**Process**" or "**Processing**" (and derivatives thereof) means any operation or set of operations performed on behalf of Controller on Personal Data or on sets of Personal Data, whether or not by automated means, such as, but not limited to, collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction, and shall be meant to include any different but similar term used in the Data Protection Laws and Regulations.

1.11 "**Processor**" means a natural or legal person, public authority, agency, or entity that Processes Personal Data on behalf of the Controller.

1.12 "**Security Documentation**" means Stream's security document, available at: https://getstream.io/security/.

1.13 "**Sensitive Data**" means (a) social security number, passport number, driver's license number, or similar identifier (or any portion thereof), (b) credit or debit card number (other than the truncated (last four digits) of a credit or debit card), (c) employment, financial, genetic, biometric or health information; (d) racial, ethnic, political or religious affiliation, trade union membership, or information about sexual life or sexual orientation; (e) account passwords; (f) date of birth; (g) criminal history; (h) mother's maiden name; and (i) any other information that falls within the definition of "special categories of data" or "sensitive data" under Data Protection Laws and Regulations.

1.14 "**Standard Contractual Clauses**" means (a) with respect to restricted transfers (as such term is understood under Data Protection Laws and Regulations) which are subject to the EU GDPR and other Data Protection Laws and Regulations pursuant to which the same have been adopted, the Controller-to-Processor standard contractual clauses or Processor to Processor standard contractual clauses (including the Swiss FDPA), as set out in the European Commission's Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to GDPR, as may be amended or replaced by the European Commission from time to time (the "**EU SCCs**"), and (b) with respect to restricted transfers subject to the UK GDPR and other Data Protection Laws and Regulations pursuant to which the EU SCCs have not been adopted, such other transfer clauses or addenda as may be adopted from time to time under the UK GDPR (including the International Data Transfer Addendum to the EU SCCs issued by the UK Information Commissioner under section 119A of the Data Protection Act 2018 (the "**UK Addendum**") and the International Data Transfer Agreement issued thereunder, in each case as revised or replaced from time to time) (collectively the "**UK SCCs**") and other Data Protection Laws and Regulations.

1.15 "**Sub-processor**" means any Processor engaged by Stream to Process Personal Data.

2. PROCESSING OF PERSONAL DATA.

2.1 Roles. Customer is the Controller and Stream is the Processor with regard to the Processing of Personal Data under the Agreement.

2.2 Customer's Processing of Personal Data. Customer shall (a) give adequate notice and make all appropriate disclosures to Data Subjects regarding Customer's use and disclosure and Stream's Processing of Personal Data, (b) obtain all necessary rights, and, where applicable, all appropriate and valid consents to disclose such Personal Data to Stream, and (c) give Stream instructions regarding the Processing of Personal Data for Customer, in all cases, in accordance with all applicable laws, rules, and regulations, including the Data Protection Laws and Regulations. Customer is solely liable and responsible for the accuracy, quality, and legality of Personal Data. Customer shall notify Stream of any determination by Customer or any changes in, or revocation of, the permission to use, disclose, or otherwise Process Personal Data that would impact Stream's ability to comply with the Agreement, or Data Protection Laws and Regulations.

2.3 Stream's Processing of Personal Data. Stream shall Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations directly applicable to Stream's provision of its Services. Personal Data shall be considered Customer's Confidential Information under the Agreement. Stream shall, unless otherwise required by law, only Process Personal Data on behalf of and in accordance with Customer's instructions set forth in this DPA and the Agreement for the following purposes: (a) Processing in accordance with the Agreement, including any Processing reasonably necessary and proportionate to achieve the business purpose outlined in the Agreement, and applicable Order Form(s); (b) Processing initiated by End Users in their use of the Services; and (c) Processing to comply with other documented reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement. Stream shall not retain, use, or disclose the Personal Data outside of the direct relationship between Stream and Customer, or outside of the purposes specified in the Agreement. Stream shall only retain, use, or disclose Personal Data as necessary for Stream's performance of its obligations under the Agreement and only in accordance with Customer's instructions. Stream shall promptly inform Customer if, in Stream's opinion, an instruction from Customer infringes Data Protection Laws and Regulations, in which case Stream may suspend performance of the affected instruction until Customer confirms, amends, or withdraws it. Stream shall not "sell" or "share" for value any Personal Data as the terms "selling" and "sharing" are defined in the CCPA. Stream shall not take any action that would cause any transfers of Personal Data to or from Stream to qualify as "selling personal information" or "sharing" under the CCPA. The subject-matter and purpose of Processing of Personal Data by Stream is solely so Stream can provide the Services to Customer pursuant to the Agreement. The duration of the Processing shall be for the duration of the Agreement. Exhibit A to this DPA identifies the nature of the Processing, the types of Personal Data Processed, and categories of Data Subjects for which data is Processed under this DPA.

2.4 Personnel. Stream shall ensure that its personnel engaged in the Processing of Personal Data are

informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements. For purposes of this Section, "personnel" includes Stream's employees and any temporary, agency, or contractor staff who have access to Personal Data. Stream shall ensure that Stream's access to Personal Data is limited to those personnel performing Services in accordance with the Agreement.

2.5 Sensitive Data. Customer will not intentionally provide (or cause to be provided) any Sensitive Data to Stream for processing under the Agreement or this DPA, and Stream will have no liability whatsoever for Sensitive Data, whether in connection with a Personal Data Incident or otherwise. If Customer nonetheless provides Sensitive Data to Stream, Stream will continue to Process such Sensitive Data subject to the protections of this DPA until it can be deleted or returned in accordance with Section 7.

2.6 U.S. State Privacy Laws. To the extent Stream Processes Personal Data subject to the CCPA or any other comprehensive United States state privacy law that constitutes a Data Protection Law and Regulation: (a) Stream acts as Customer's "service provider," "contractor," or "processor" (as applicable under such law), and Customer discloses Personal Data to Stream solely for the limited and specified business purposes described in Section 2.3 and the Agreement (which the parties shall describe specifically, and not in generic terms or by general reference to the entire Agreement, in the Agreement, the applicable Order Form, or Exhibit A); (b) Stream shall not combine Personal Data it receives from or on behalf of Customer with personal information that it receives from or on behalf of any other person or collects from its own interactions with individuals, except as permitted for service providers, contractors, or processors under such laws; (c) Stream shall comply with the obligations applicable to it under such laws and shall provide the same level of privacy protection as such laws require of Customer; (d) Stream shall notify Customer if Stream determines that it can no longer meet its obligations under such laws; (e) Customer may take reasonable and appropriate steps, including through the audit rights in Section 8, to help ensure that Stream uses Personal Data in a manner consistent with Customer's obligations under such laws and, upon notice to Stream, to stop and remediate any unauthorized use of Personal Data; (f) taking into account the nature of the Processing and the information available to Stream, Stream shall provide reasonable assistance to Customer in meeting Customer's obligations under such laws to complete Customer's cybersecurity audit, to conduct risk or data protection assessments, and to comply with requirements regarding automated decision-making technology, in each case to the extent required by such laws and subject to Section 3 with respect to costs; (g) the nature and purpose of the Processing, the type of Personal Data, the categories of Data Subjects, and the duration of the Processing are as set forth in the Agreement, this DPA, and Section B to Exhibit A, and Stream's obligations regarding confidentiality, Sub-processors, return and deletion, and audits are set forth in Sections 2.4, 4, 7, and 8, respectively; and (h) to the extent Stream acts as a "contractor" under such laws, Stream certifies that it understands the restrictions set forth in this Section 2.6 and the applicable law and will comply with them.

3. RIGHTS OF DATA SUBJECTS. Stream shall, to the extent legally permitted, promptly notify Customer if Stream receives a request from a Data Subject to exercise the Data Subject's rights under Data Protection Laws and Regulations ("**Data Subject Request**"). Taking into account the nature of the Processing, Stream shall assist Customer by maintaining appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. In addition, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, Stream shall upon Customer's request provide reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent Stream is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws and Regulations. Taking into account the nature of the Processing and the information available to Stream, Stream shall also provide reasonable assistance to Customer with data protection impact assessments and prior consultations with supervisory authorities where required under European Data Protection Laws. To the extent legally permitted, Customer shall be responsible for any costs arising from Stream's provision of such assistance.

4. SUB-PROCESSORS.

4.1 Appointment of Sub-processors. Customer acknowledges and agrees that Stream may engage third-party Sub-processors in connection with the provision of the Services. Stream has entered into a written agreement with each Sub-processor containing data protection obligations not less protective than those in this DPA with respect to the protection of Personal Data to the extent applicable to the nature of the Services provided by such Sub-processor.

4.2 List of Current Sub-processors. Stream's current list of Sub-processors for the Services is available at https://getstream.io/legal/subprocessors/ (the "**Sub-processor List**"), which Customer hereby approves and authorizes. Stream may engage additional Sub-processors as Stream considers reasonably appropriate for the Processing of Personal Data in accordance with this DPA, provided that Stream shall notify Customer of the

addition or replacement of any Sub-processor, by email or another active notification mechanism to which Customer may subscribe, a reasonable period before the new or replacement Sub-processor begins Processing Personal Data.

4.3 Objection Right for New Sub-processors. Customer may object to Stream's use of a new Sub-processor by notifying Stream promptly in writing within thirty (30) days after Stream's notice of the new Sub-processor under Section 4.2, giving reasons for Customer's objection. Customer's failure to object within such thirty (30) day period shall be deemed Customer's waiver of its right to object to Stream's use of a new Sub-processor added to the Sub-processor List. In the event Customer objects to a new Sub- processor, Stream will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening the Customer. If Stream is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Customer may terminate the applicable Order Form(s) with respect only to those Services which cannot be provided by Stream without the use of the objected-to new Sub-processor by providing written notice to Stream.

4.4 Liability. Stream shall be liable for the acts and omissions of its Sub-processors to the same extent Stream would be liable if performing the Services of each Sub-processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

5. SECURITY. Stream shall maintain, during the term of the Agreement, appropriate technical and organizational security measures to protect the Personal Data against accidental or unlawful destruction or accidental loss, damage, alteration, unauthorized disclosure or access, as set forth in Exhibit B (the "**Security Measures**"). Stream's Security Measures will include those set forth in the Security Documentation and will be aligned to the ISO/IEC 27001 standard for information security management. Stream regularly monitors compliance with these measures and annually performs a SOC 2 Type II compliance audit. Stream shall provide Customer with a copy of any ISO/IEC 27001 or SOC 2 Type II audit report obtained by Stream upon request. Stream will not materially decrease the overall Security Measures of the Services during a subscription term.

6. CUSTOMER DATA INCIDENT MANAGEMENT AND NOTIFICATION. Stream maintains security incident management policies and procedures specified in the Security Documentation and shall notify Customer without undue delay, but in no event later than 72 hours, after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise Processed by Stream (a "**Personal Data Incident**"). Stream's notification will include, to the extent then known and taking into account the information available to Stream, a description of the nature of the Personal Data Incident, the categories and approximate number of Data Subjects and records concerned, the likely consequences, and the measures taken or proposed to address it, in order to assist Customer in meeting its obligations under Articles 33 and 34 of the GDPR and any analogous obligations under Data Protection Laws and Regulations. Stream shall make reasonable efforts to identify the cause of such Personal Data Incident and take those steps pursuant to applicable Data Protection Laws and Regulations as Stream deems necessary and reasonable in order to remediate the cause of such a Personal Data Incident to the extent the remediation is within Stream's reasonable control. The obligations herein shall not apply to a Personal Data Incident that is caused by an act or omission of Customer or Customer's End Users.

7. RETURN AND DELETION OF CUSTOMER DATA. If Customer cannot access or delete its Personal Data through the self-service functionalities of the Services provided by Stream under the Agreement, Stream shall, at Customer's election, return to Customer or delete the Personal Data, and delete existing copies, unless retention of the Personal Data is required by applicable law, within a reasonable period not to exceed sixty (60) days following the end of the provision of the Services. Customer shall make use of self-service functionalities before requesting Stream for assistance.

8. RELEVANT RECORDS AND AUDIT RIGHTS. Customer may audit Stream's compliance with its obligations under this DPA up to once per year and on such other occasions as may be required by Data Protection Laws and Regulations. Stream will allow for and contribute to such audits by providing Customer or Customer's supervisory authority with the information and assistance reasonably necessary to demonstrate compliance with this DPA and to conduct the audit. To request an audit, Customer must submit a proposed audit plan to Stream at least twenty (20) days in advance of the proposed audit date and any third-party auditor must sign a customary non-disclosure agreement mutually acceptable to the parties (such acceptance not to be unreasonably withheld) providing for the confidential treatment of all information exchanged in connection with the audit and any reports regarding the results or findings thereof. The proposed audit plan must describe the proposed scope, duration, and start date of the audit. Stream will review the proposed audit plan and provide Customer with any concerns or questions (for example, any request for information that could compromise Stream security, privacy, employment

or other relevant policies). Stream will work cooperatively with Customer to agree on a final audit plan. Nothing in this Section 8 shall require Stream to breach any duties of confidentiality. If the controls or measures to be assessed in the requested audit are addressed in a SOC 2 Type 2, ISO, NIST or similar audit report performed by a qualified third-party auditor within twelve (12) months of Customer's audit request and Stream has confirmed there have been no known material changes in the controls audited since the date of such report, Customer agrees to accept such report in lieu of requesting an audit of such controls or measures. The audit must be conducted during regular business hours, subject to the agreed final audit plan and Stream's safety, security or other relevant policies, and may not unreasonably interfere with Stream business activities. Any audits are at Customer's sole expense. Customer shall reimburse Stream for reasonable time expended by Stream in connection with any Customer-requested audit or inspection under this Section 8 at Stream's then-current professional services rates, which shall be made available to Customer upon request, provided that such charges shall not be set so as to make the exercise of Customer's audit rights impracticable. Customer will be responsible for any fees charged by any auditor appointed by Customer to execute any such audit.

9. CHANGES. Stream may change this DPA unless the Data Protection Laws and Regulations prohibit Stream from making such change without explicit agreement from Customer; provided that Stream shall not unilaterally amend the Standard Contractual Clauses except to conform them to new or replacement clauses adopted by the European Commission or the UK Information Commissioner, or to incorporate supplementary safeguards that do not contradict the Standard Contractual Clauses or reduce the level of protection they afford.

10. INTERNATIONAL DATA TRANSFER.

10.1 Data Processing Facilities. Stream may, subject to this Section 10, Process Personal Data in the United States or anywhere Stream or its Sub-processors maintains facilities. Subject to Stream's obligations in this Section 10, Customer is responsible for ensuring that its use of the Services comply with any cross-border data transfer restrictions of Data Protection Laws and Regulations.

10.2 Data Protection Framework. Stream has certified to the U.S. Department of Commerce that it adheres to the principles of the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, and the Swiss-U.S. Data Privacy Framework (all such Data Privacy Frameworks, the "**DPFs**") as set forth by the U.S. Department of Commerce. To the extent the DPFs provide a means of transfer of Personal Data subject to European Data Protection Laws from the European Union / European Economic Area, the United Kingdom (and Gibraltar), and/or Switzerland to the United States, such transfer will be subject to the DPFs, and related principles, as permitted thereunder. Notwithstanding the foregoing, if any of the DPFs, or any adequacy decision on which a DPF relies, is invalidated, suspended, or otherwise ceases to be a valid means of transferring Personal Data, or if Stream's certification under a DPF lapses or is withdrawn, then, effective from the date on which such DPF ceases to apply to the relevant transfer and without any further action by the parties, the Standard Contractual Clauses shall apply to such transfer in accordance with Section 10.3.

10.3 Standard Contractual Clauses. In the event that Customer transfers Personal Data subject to European Data Protection Laws to Stream in a country which has not been recognized as providing an adequate level of protection for such Personal Data within the meaning of applicable European Data Protection Laws, and no lawful alternative basis, mechanism, or framework for such transfer of Personal Data applies, such transfer will be governed by the Standard Contractual Clauses, the terms of which are hereby incorporated into this DPA. For the avoidance of doubt: (a) if Customer is acting as the Controller with respect to Personal Data, "Module Two: Transfer controller to processor" shall apply; or (b) if Customer is acting as a Processor to a third-party Controller with respect to Personal Data, "Module Three: Transfer processor to processor" shall apply. The Standard Contractual Clauses shall automatically terminate once the Personal Data transfer governed thereby becomes lawful under European Data Protection Laws in the absence of such Standard Contractual Clauses on any other basis. Notwithstanding the foregoing, the Standard Contractual Clauses (including the EU SCCs and UK SCCs) (or obligations the same as those under the Standard Contractual Clauses) will not apply to the extent an alternative recognized compliance standard for the transfer of Personal Data outside the EEA, Switzerland, or the UK in accordance with Data Protection Laws and Regulations applies to the transfer. Stream shall provide a copy of the EU SCCs and/or UK SCCs, as applicable, to Customer upon request. Where the Standard Contractual Clauses apply, the parties will cooperate in good faith to carry out and document any transfer impact assessment or transfer risk assessment required under European Data Protection Laws, with Stream, as data importer, providing information within its knowledge regarding the laws and practices of the destination country relevant to the transfer.

10.4 Transfers out of the EEA or Switzerland. To the extent the EU SCCs are applicable to transfers of Personal Data to the United States pursuant to Section 10.3, the parties agree as follows:

(a) Customer will act as the data exporter and Stream will act as the data importer under the EU SCCs;

(b) for purposes of Appendix 1 to the EU SCCs, the categories of data subjects, data, special categories of data (if appropriate), and the Processing operations shall be as set out in Section B to Exhibit A;

(c) for purposes of Appendix 2 to the EU SCCs, the technical and organizational measures shall be the Security Measures;

(d) in Clause 7 (Docking Clause), the optional docking clause will not apply;

(e) the audits described in Clause 8.9 of the EU SCCs shall be performed in accordance with Section 8 of this DPA;

(f) Option 1 in Clause 9 is struck and Option 2 is kept, and data importer will submit the specific information in accordance with Section 4.2 of this DPA;

(g) in Clause 11 (Redress), the optional language will not apply;

(h) Option 1 of Clause 17 (Governing law) shall apply and the governing law shall be the law of the Republic of Ireland. In accordance with Clause 18(b) (Choice of forum and jurisdiction), any dispute arising from the EU SCCs shall be resolved by the courts of the Republic of Ireland; and

(i) For Switzerland, the term 'Member State' will be interpreted in such a way as to allow data subjects in Switzerland to exercise their rights under the Clauses in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the EU SCCs.

10.5 Transfers out of the UK. To the extent the UK SCCs are applicable to transfers of Personal Data to the United States pursuant to Section 10.3, the UK SCCs are clarified to the extent the EU SCCs are clarified pursuant to Section 10.3 and Section 10.4, if and as permissible under the UK GDPR. To the extent the UK Addendum applies, the EU SCCs, as completed in accordance with Section 10.4 and Exhibits A through C, shall constitute the "Approved EU SCCs" for purposes of the UK Addendum, and Tables 1 through 3 of the UK Addendum shall be deemed completed with the corresponding information set out in Exhibits A through C. In furtherance of the foregoing, the parties agree that:

(a) Customer will act as the data exporter and Stream will act as the data importer under the UK SCCs;

(b) for purposes of Appendix 1 to the UK SCCs, the categories of data subjects, data, special categories of data (if appropriate), and the Processing operations shall be as set out in Section B to Exhibit A; and

(c) for purposes of Appendix 2 to the UK SCCs, the technical and organizational measures shall be the Security Measures.

11. CLAIMS. Any claims brought under, or in connection with, this DPA, shall be subject to the exclusions and limitations of liability set forth in the Agreement.

Exhibit A

A. LIST OF PARTIES

Data exporter(s):

Name:	Customer
Address:	As specified in the Agreement or the Order Form.
Contact person's name, position and contact details:	Contact details for the data exporter are specified in the Agreement or the Order Form.
Activities relevant to the data transferred under these Clauses:	Receipt of data importer's Services under the Agreement or the Order.
Signature and Date:	The parties agree that execution of the Agreement by the data exporter and the data importer shall constitute execution of these Clauses by both parties as of the effective date listed in the Order Form.
Role (controller/processor):	Controller (if Module Two applies) or processor (if Module Three applies)

Data importer(s):

Name:	Stream.io, Inc.
Address:	1215 Spruce Street Suite 300, Boulder, CO 80302
Contact person's name, position and contact details:	Thierry Schellenbach, CEO, thierry@getstream.io
Activities relevant to the data transferred under these Clauses:	Receipt of data importer's Services under the Agreement or the Order.
Signature and Date:	The parties agree that execution of the Agreement by the data exporter and the data importer shall constitute execution of these Clauses by both parties as of the effective date listed in the Order Form.
Role (controller/processor):	Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred	Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects: ● Prospects, customers, business partners and vendors of Customer (who are natural persons) ● Employees or contact persons of Customer's prospects, customers, business partners and vendors ● Employees, agents, advisors, freelancers of Customer (who are natural persons) ● Customer's End Users authorized by Customer to use the Services

Categories of personal data transferred	Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data: ● First and last name ● Title ● Position ● Employer ● Contact information (company, email, phone, physical business address) ● ID data ● Professional life data ● Personal life data ● Connection data ● Localization data
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 specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.	N/A
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).	Continuous basis during the term of the Agreement.
Nature of the processing	As described in the Agreement and any Order Form.
Purpose(s) of the data transfer and further processing	As described in the Agreement and any Order Form.
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period	Duration of performance of the Services, except as required by applicable law.
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing	As described in the Agreement and any Order Form.

C. COMPETENT SUPERVISORY AUTHORITY

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

Netherlands
Autoriteit Persoonsgegevens
Bezuidenhoutseweg 30
P.O. Box 93374
2509 AJ Den Haag/The Hague Tel. +31
70 888 8500
Fax +31 70 888 8501
Website: https://autoriteitpersoonsgegevens.nl/

The above supervisory authority shall apply unless otherwise agreed by the parties as mandated by the established rules of selection of the relevant supervisory authority, or Sections 2 or 3 of the attached DPA apply.

Exhibit B

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

1. Stream has implemented and will maintain a comprehensive written information security program that contains technical and organisational safeguards, which shall at a minimum contain those safeguards described at: https://getstream.io/security/. Additionally, Stream can provide ISO/IEC 27001 and SOC 2 Type II reports upon request. For the avoidance of doubt, Stream maintains the following security measures:

A. Organizational management and dedicated staff responsible for the development, implementation and maintenance of the Stream's information security program.

B. Audit and risk assessment procedures for the purposes of periodic review and assessment of risks to Stream's organization, monitoring and maintaining compliance with the Stream's policies and procedures, and reporting the condition of its information security and compliance to internal senior management.

C. Data security controls which include, at a minimum, logical segregation of data, restricted (e.g. role- based) access and monitoring, and utilization of commercially available industry standard encryption technologies for Personal Data that is transmitted over public networks (i.e. the Internet) or when transmitted wirelessly or at rest or stored on portable media (i.e. laptop computers).

D. Logical access controls designed to manage electronic access to data and system functionality based on authority levels and job functions, (e.g. granting access on a need-to-know and least privilege basis, use of unique IDs and passwords for all users, periodic review and revoking/changing access promptly when employment terminates or changes in job functions occur).

E. Password controls designed to manage and control password strength, expiration and usage including prohibiting users from sharing passwords and requiring that the Stream's passwords that are assigned to its employees: (i) be at least twelve (12) characters in length, (ii) not be stored in readable format on the Stream's computer systems; (iii) must have defined complexity; (iv) newly issued passwords must be changed after first use; and (v) multi-factor authentication is required for remote and administrative access to systems containing Personal Data.

F. System audit or event logging and related monitoring procedures to proactively record user access and system activity.

G. Physical and environmental security of data centers, server room facilities and other areas containing Personal Data designed to: (i) protect information assets from unauthorized physical access, (ii) manage, monitor and log movement of persons into and out of the Stream's facilities, and (iii) guard against environmental hazards such as heat, fire and water damage.

H. Operational procedures and controls to provide for configuration, monitoring and maintenance of technology and information systems, including secure disposal of systems and media to render all information or data contained therein as undecipherable or unrecoverable prior to final disposal or release from the Stream's possession.

I. Change management procedures and tracking mechanisms designed to test, approve and monitor all material changes to the Stream's technology and information assets.

J. Incident management procedures designed to allow Stream to investigate, respond to, mitigate and notify of events related to the Stream's technology and information assets.

K. Network security controls designed to protect systems from intrusion and limit the scope of any successful attack.

L. Vulnerability assessment, patch management and threat protection technologies, and scheduled monitoring procedures designed to identify, assess, mitigate and protect against identified security threats, viruses and other malicious code.

M. Disaster recovery procedures designed to maintain service and/or recovery from foreseeable emergencies or disasters.

Exhibit C

List of Sub-processors

The controller has authorized the use of the following Sub-processors:

Stream's current list of Sub-processors for the Services is available at https://getstream.io/legal/subprocessors/.