Mux, Inc.
Data Processing Addendum

Updated April 1, 2025

This Mux, Inc. Data Processing Addendum including its Annexes (the "**DPA**") is entered by and between Mux, Inc., 50 Beale Street, 9th Floor San Francisco, CA 94105 ("**Mux**") and the Mux customer identified in a respective order form ("**Customer**") pursuant to the Master Services Agreement, the Mux Terms of Service, or other written or electronic agreement between the parties governing the Services (as applicable) ("**Agreement**"). Each party is herein referred to individually as a "**Party**," or collectively as the "**Parties**".

This DPA forms part of the Agreement and sets out the terms that apply when Personal Data (as defined below) is processed by Mux on behalf of Customer in performance of the Services under the Agreement. The purpose of the DPA is to ensure such processing is conducted in accordance with applicable laws and with due respect for the rights and freedoms of individuals whose Personal Data is processed.

1. DEFINITIONS

Any capitalized term used but not defined in this DPA has the meaning provided to it under Applicable Law or in the Agreement.

1.1 "**Affiliate**" means an entity that, directly or indirectly, owns or controls, is owned or is controlled by, or is under common ownership or control with Customer and who is a beneficiary under the Agreement, or any order form based thereon.

1.2 "**Applicable Law**" means all laws, rules, and regulations applicable to Mux's processing of Personal Data under the Agreement, including but not limited to (a) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (General Data Protection Regulation ("**GDPR**"), (b) in respect of the UK, the GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 ("**UK GDPR**") and the Data Protection Act 2018 (together, "**UK Data Protection Laws**"), (c) the Swiss Federal Data Protection Act and its implementing regulations ("**Swiss DPA**"), (d) CCPA (as defined below) and other state consumer protection laws that apply to the processing of Personal Data by Mux hereunder; in each case with respect to (a)-(d) above, as may be amended, superseded or replaced.

1.3 "**CCPA**" means the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 and as further amended (Cal. Civ. Code §§ 1798.100 et seq.) and any binding regulations promulgated thereunder, in each case, as may be amended from time to time.

1.4 "**Personal Data**" means any information relating to an identified or identifiable natural person ("data subject") that Mux processes on behalf of Customer pursuant to its performance of the Services under the Agreement, or as may be similarly identified or defined under Applicable Law including but not limited to "personal information", "personally identified information" or its equivalent.

1.5 "**Privacy Policy**" means the then-current privacy policy for the Services available at Privacy Policy | Mux.

1.6 “**Restricted Transfer**” means (i) where the GDPR applies, a transfer of Personal Data from the European Economic Area to a country outside of the European Economic Area which is not subject to an adequacy determination by the European Commission; (ii) where the UK GDPR applies, a transfer of Personal Data from the UK to any other country which is not based on adequacy regulations pursuant to Section 17A of the Data Protection Act 2018; and (iii) where the Swiss DPA applies, a transfer of Personal Data to a country outside of Switzerland which is not included on the list of adequate jurisdictions published by the Swiss Federal Data Protection and Information Commissioner.

1.7 “**Security Breach**” means an actual breach of security leading to any accidental, unauthorized or unlawful loss, disclosure, destruction, loss, alteration, or access to Personal Data transmitted, stored or otherwise processed by Mux. A Security Breach shall not include an unsuccessful attempt or activity that does not compromise the security of Personal Data, including (without limitation) pings and other broadcast attacks of firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers) or similar incidents.

1.8 "**Sell**" shall have the meaning given in the CCPA.

1.9 “**Standard Contractual Clauses**” or "**SCCs**" means (i) where the GDPR applies, the standard contractual clauses annexed to the European Commission's Implementing Decision (EU) 2021/914 of 4 June 2021 standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914&from=EN ("EU SCCs"); (ii) where the UK GDPR applies, the applicable standard data protection clauses adopted pursuant to Article 46(2)(c) or (d) of the UK GDPR, where the UK GDPR means the International Data Transfer Addendum to the EU Standard Contractual Clauses issued by the Information Commissioner's Office under s.119A(1) of the Data Protection Act 2018, as such Addendum may be revised under Section 18 therein ("UK SCCs") and (iii) where the Swiss DPA applies, the applicable standard data protection clauses issued, approved or recognized by the Swiss Federal Data Protection and Information Commissioner (the "Swiss SCCs") (in each case, as updated, amended or superseded from time to time).

1.10 The terms “Business”, "Controller", "Data Subject", "Process", "Processor", “Service Provider”, "Sub-Processor” and "Supervisory Authority" shall have the same meaning as set out under Applicable Law.

2. APPLICABILITY & SCOPE

2.1 This DPA will apply only to the extent that Mux processes, on behalf of Customer, Personal Data to which Applicable Law applies to Mux’s processing of such Personal Data.

2.2 The subject matter of the processing is the provision of the Services, and the processing will be carried out for the duration of the Agreement. **Exhibit 1 (Details of Processing)** sets out details including but not limited to the nature and purpose of the processing and the categories of Personal Data and data subjects whose Personal Data is processed by Mux.

2.3 In the course of providing the Services, Mux may process Personal Data of (i) Customer, (ii) its Affiliates, and/or (iii) Customer’s customers (collectively, "**Customer’s Customers**").

2.4 The parties acknowledge and agree that regarding the processing of Personal Data, Customer may act either as a Controller or Processor and Mux is a Processor or Sub processor to Customer. Mux will process Personal Data in accordance with Customer's instructions as set forth in Section 4 below.

3. DETAILS OF DATA PROCESSING

3.1 Mux will process Personal Data in order to provide the Services in accordance with the terms of the Agreement. **Exhibit 1 (Details of Processing)** of the DPA further specifies the nature and purpose of the processing, processing activities, duration of processing, categories of Personal Data and data subjects.

4. CUSTOMER'S OBLIGATIONS

4.1 Customer Instructions. Customer appoints Mux as a processor to process Personal Data on behalf of, and in accordance with, Customer's instructions (a) as set forth in the Agreement, this DPA, and as otherwise necessary to provide the Services to Customer (which may include investigating security breaches and detecting and preventing exploits or abuse); (b) as necessary to comply with Applicable Law; and (c) as otherwise agreed in writing between the parties. Mux will inform Customer if it becomes aware, or reasonably believes, that Customer's instructions violate Applicable Law.

4.2 Lawfulness of Instructions. Customer will ensure that its instructions comply with Applicable Law. Customer acknowledges that Mux is neither responsible for determining which laws are applicable to Customer's business nor whether Mux's Services meet or will meet the requirements of such laws. Customer will ensure that Mux's processing of Personal Data, when done in accordance with Customer's instructions, will not cause Mux to violate any Applicable Law. Customer shall inform Mux immediately if its instructions to Mux might lead to a violation of Applicable Law.

4.3 Additional Instructions. Additional instructions outside the scope of the Agreement or this DPA will be mutually agreed to between the Parties in writing.

4.4 Customer shall be responsible for ensuring that: a) all such notices have been given, and all such authorizations have been obtained, as required under Applicable Law, for Mux (and its Affiliates and Sub-processors) to process Personal Data as contemplated by the Agreement and this DPA; b) it has complied, and will continue to comply, with all laws relating to Customer's privacy and data protection obligations, including Applicable Laws; and c) it has, and will continue to have, the right to transfer, provide access to, or authorize Mux to collect Personal Data in accordance with the terms of the Agreement and this DPA.

4.5 With respect to Affiliates, by signing this DPA Customer warrants it is duly authorized:

4.5.1 to enter into this DPA for and on behalf of any such Affiliates;

4.5.2 to enforce the terms of this DPA on behalf of the Affiliates, and to act on behalf of the Affiliates in the administration and conduct of any claims arising in connection with this DPA; and

4.5.3 to receive and respond to any notices or communications under this DPA on behalf of Affiliates.

4.6 Subject to Section 4.5, each Affiliate shall be bound by this DPA as if it was the Customer, unless this DPA differentiates between the Customer and its Affiliates, in which case the specific provision shall prevail.

4.7 With regard to cases under Section 2.3(iii) Customer warrants that it (i) is authorized by Customer's Customers to enter into this DPA as their processor as well as to engage Mux as their sub-processor

and (ii) has concluded appropriate data processing agreements with its Customer's Customers as the controller. Since the Customer is the only Party which has a direct relationship with Customer's Customers, the Parties agree that any rights under this DPA granted to Customer's Customer shall be exercised through Customer.

4.8 The parties agree that any notice or communication sent by Mux to Customer shall also satisfy any obligation to send such notice or communication to Customer's Affiliates and/or Customer's Customers and Customer agrees to promptly forward all notifications as applicable hereunder.

5. SECURITY

5.1 Mux has in place and will maintain throughout the term of this DPA appropriate technical and organizational measures designed to protect Personal Data. Such measures shall at a minimum comply with Applicable Law and include the measures which are described in **Exhibit 2, Technical and Organizational Security Measures**.

5.2 Customer understands that the security measures are subject to technical progress and development and that Mux may update or modify the security measures from time to time, provided that such updates and/or modifications do not result in the degradation of the overall security of the Services or noncompliance with Applicable Law.

5.3 Upon written request, Mux shall make available to Customer a description of Mux's current security measures to enable Customer to assess compliance with Applicable Law and this DPA.

5.4 Mux will ensure that any person authorized to process Personal Data (including its staff, agents and subcontractors) shall be subject to a binding duty of confidentiality.

5.5 Mux shall notify Customer in writing without undue delay, and in no event more than seventy-two (72) hours after becoming aware of any Security Breach and shall reasonably cooperate in the investigation of any such Security Breach in accordance with Applicable Law. Mux shall not make any statement or disclosure to the public, any governmental entity or any other third party about a Security Breach that references Customer or from which Customer's involvement could be reasonably inferred, except as required by Applicable Law or with Customer's prior written consent.

5.6 In the event any request is made by a third party directly to Mux in connection with Mux's processing of Personal Data, Mux will promptly inform Customer and provide details of the same, to the extent legally permitted. Mux will not respond to any third party request, without prior notice to Customer and an opportunity to object, except: (i) as legally required to do so, (ii) to confirm that such third party request relates to Customer, or (iii) to inform the respective third party that Mux is not the owner of the Personal Data but merely the Processor or Sub-processor.

6. AUDITS

6.1 In order to comply with its obligation to make available all information to demonstrate compliance in accordance with Applicable Law, Mux shall, upon written request and subject to an appropriate non-disclosure agreement, provide to Customer comprehensive documentation of its technical and organizational measures in accordance with industry standards and Applicable Law. The effectiveness of Mux's technical and organizational measures will be audited by an independent third-party engaged by Mux on a regular basis. In addition, Mux may, in its discretion, provide data

protection compliance certifications issued by a commonly accepted certification issuer which has been audited by a data security expert, by a publicly certified auditing company, or by another customer of Mux.

6.2 In accordance with Applicable Law, Mux will allow for and contribute to audits of Mux's compliance with its obligations under this DPA once annually. In addition, Customer may perform more frequent audits in the event Mux experiences a Security Breach and Customer has already requested an audit within the prior twelve (12) months or as required by Applicable Law. Where Customer engages a third-party to conduct such audit, Customer agrees to require such third-party to execute Mux's non-disclosure agreement. Customer agrees to comply and agrees to require any third party auditor engaged by Customer to comply with Mux's policies and procedures when performing the audit, including but not limited to Mux's information security, confidentiality, and visitor access policies. The costs associated with such audits and/or for providing additional information shall be borne by Customer, unless such audit is due to or reveals Mux's material breach of this DPA.

6.3 The aforementioned audit right can be exercised by (i) requesting additional information, (ii) accessing the databases which process Personal Data or (iii) by inspecting Mux's working premises whereby in each case Customer understands that no access to personal data of other customers or Mux's Confidential Information will be granted.

6.4 If Customer intends to conduct an audit at Mux's premises or physical facilities, Mux will allow for such audits in accordance with Applicable Law, and Customer shall provide no less than thirty (30) days advance written notice to Mux and the parties shall mutually agree on the details, time and duration of the audit and inspections to take place during regular business hours and in such a way that business operations are not disturbed. At least one employee of Mux must always accompany the auditors. All results of the audit shall be deemed Confidential Information of Mux.

6.5 With respect to third party auditors engaged by Customer to perform the audit in accordance with the terms of this DPA on its behalf, Customer may not appoint a third party as auditor who (i) Mux reasonably considers to be in a competitive relationship to Mux, or (ii) is not sufficiently qualified to conduct such an audit, or (iii) is not independent. Any expenses incurred by an auditor in connection with an audit including the review of any reports shall be borne by Customer.

6.6 For clarity, the exercise of audit rights under the SCCs shall be as described in this Section 6 (Audits).

7. SUBPROCESSORS

7.1 In accordance with Applicable Law, Mux has Customer's and/or Customer's Customers general authorization for the engagement of sub-processor(s) necessary to perform the Services under the Agreement as set out in **Exhibit 3, Mux SubProcessors** and as may be updated from time to time.

7.2 Such general authorization is conditioned on the following requirements: (a) Mux will restrict the sub-processors access to Personal Data only to what is strictly necessary to provide the Services, (b) all sub-processors shall be required to commit to data protection obligations, including appropriate technical and organizational measures to protect Personal Data, appropriate for their level of access to and/or scope of processing of Personal Data on behalf of Mux hereunder, and (c) Mux shall

remain responsible for the acts and omissions of its Sub-processors as if they were the acts and/or omissions of Mux hereunder.

7.3 In order to fulfil its obligation under this section, Mux may provide a website or provide another written notice that lists all sub-processors who may have access to Personal Data as well as the services they perform. In accordance with Applicable Law, Mux will update its website and/or notify Customer in light of any change of sub-processors at least thirty (30) days before authorizing any new sub-processor to access personal data, whereas (as applicable) Customer will immediately forward such notification to Customer's Customers and thereby grant Customer and Customer's Customers the opportunity to object. After issuance of the notice required hereunder, the change in the sub-processing shall be deemed as accepted unless Customer objects (on behalf of itself or Customer's Customer) within fourteen (14) days to Mux in writing. In the case that Customer object/s to the change of sub-processors, Customer shall provide documentary evidence that reasonably shows, or reasons why there is a reasonable belief that the Sub-processor does not or cannot comply with Applicable Law related to the processing of Personal Data. Mux will use reasonable efforts to refrain from permitting such proposed Sub-processor to process Personal Data without adversely impacting the Services. If Mux determines that it cannot avoid such an adverse impact despite such reasonable efforts, Mux shall notify Customer of such determination no later than fourteen (14) days after receipt of Customer's objection. Upon receipt of such notice, Customer may terminate the portion of the Agreement relating to the affected Service without penalty or liability (other than for fees due and owing to Mux for Services performed prior to such termination) effective immediately upon written notice of such termination to Mux. Mux shall refund Customer any prepaid fees for the period following the effective date of termination.

8. DATA SUBJECT REQUESTS

8.1 In the event a data subject requests to exercise a right available under Applicable Law directly to Mux, Customer hereby instructs Mux, to the extent Mux is able to identify through reasonable means the Customer as the Controller of the Personal Data, to refer the data subject to Customer, who will, as applicable, either respond to such request within the time period prescribed by Applicable Law or refer the data subject to Customer's Customer.

8.2 Upon Customer's written request, Mux shall, taking into account the nature of the processing, provide reasonable cooperation and assistance to Customer where possible and at Customer's cost and expense, to enable Customer to respond to requests from a data subject seeking to exercise their rights under Applicable Law.

8.3 As between the parties, Customer shall have sole discretion and responsibility in responding to the rights asserted by any individual in relation to their Personal Data.

9. SUPPORT AND COOPERATION

Mux undertakes to provide reasonable support to Customer to ensure compliance with the requirements imposed by Applicable Law that require operational details related to the processing of Personal Data or organizational and technical measures in place to protect it. In accordance with and as required by Applicable Law, Mux will do so, in particular, by providing information to Customer which is reasonably necessary for Customer to complete a transfer impact assessment ("**TIA**") or

other data protection impact assessments or consultations with data protection authorities that Customer is required to carry out under such legislation, at Customer's cost and expense.

10. TRANSFER MECHANISM

10.1 Location of Processing. Customer acknowledges that Mux and its Sub-processors may transfer and process Personal Data to and in the United States of America and other locations in which Mux, its Affiliates or its Sub-processors maintain data processing operations, as more particularly described in **Exhibit 3**. Mux shall ensure that such transfers are made in compliance with Applicable Law and this DPA.

10.2 Transfer Mechanism. The parties agree that when the transfer of Personal Data from Customer (as "data exporter") to Mux (as "data importer") is a Restricted Transfer, Applicable Law requires that appropriate safeguards are put in place. For the purposes of such Restricted Transfers from Customer to Mux, the parties rely on Mux's certification under the EU-US Data Privacy Framework, the Swiss-US Data Privacy Framework and the UK-US Data Privacy Framework (together, the "DPF") operated by the U.S. Department of Commerce. To the extent that the DPF is invalidated or ceases to be an appropriate safeguard under Article 46 GDPR for transfers of Personal Data to the United States, then, such transfer shall be subject to the appropriate Standard Contractual Clauses, which shall be deemed incorporated into and form part of this DPA, as follows:

10.2.1 In relation to transfers of Personal Data that is protected by the GDPR, the EU SCCs shall apply, completed as follows:

(a) Module Two: Transfer controller to processor; "SCC Controller to Processor", and/or Module Three: Transfer processor to processor; "SCC Processor to Processor" and both Modules referred to as "SCC" will apply (as applicable)

(b) in Clause 7, the optional docking clause shall not apply;

(c) in Clause 9, Option 2 will apply; for Module 2, the time period for prior notice of Sub-processor changes shall be as set out in Section 7 of this DPA, and for Module 3, the time period for prior notice shall be 14-days;

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

(e) in Clause 17, Option 1 will apply, and the EU SCCs will be governed by the law of the Republic of Ireland;

(f) in Clause 18(b), disputes shall be resolved before the courts of Republic of Ireland;

(g) Annex I of the EU SCCs shall be deemed completed with the information set out in Exhibit 1 to this DPA; and

(h) Subject to Section 5 of this DPA, Annex II of the EU SCCs shall be deemed completed with the information set out in Exhibit 2 to this DPA;

10.2.2 In relation to transfers of personal data protected by the UK GDPR or Swiss DPA, the EU SCCs as implemented under sub-paragraphs (a) and (b) above will apply except as modified by the terms of the **UK and Swiss Addendum** at **Exhibit 4**, the terms of which are incorporated herein.

10.2.3 It is not the intention of either party to contradict or restrict any of the provisions set forth in the Standard Contractual Clauses and, accordingly, if and to the extent the Standard Contractual Clauses conflict with any provision of the Agreement (including this DPA) the Standard Contractual Clauses shall prevail to the extent of such conflict.

10.3 Alternative Transfer Mechanism. To the extent that Mux adopts an alternative data export mechanism (including any new version of or successor to the DPF or Standard Contractual Clauses adopted pursuant to Applicable Law) ("**Alternative Transfer Mechanism**"), the Alternative Transfer Mechanism shall, upon notice to Customer and provided it complies with Applicable Law, apply instead of any applicable transfer mechanism described in this DPA.

11. California Consumer Privacy Act

For purposes of the CCPA, the following provisions are intended to supplement and/or clarify the terms and conditions of this DPA to the extent the DPA terms do not already cover the CCPA requirements:

11.1.1 Customer's Role. Customer will act as a "**Business**" and thus will determine the purpose and means of processing Personal Data. Customer will provide Personal Data to Mux solely for the purpose of Mux performing the Services.

11.1.2 Mux's Role. Mux will act as a "**Service Provider**" in its performance of its obligations pursuant to the Agreement.

11.1.3 Disclosure of Personal Data. Mux shall not Sell, share, disclose, release, transfer, make available or otherwise communicate any Personal Data to another business or third party without the prior written consent of Customer. Notwithstanding the foregoing, nothing in this DPA shall restrict Mux's ability to disclose Personal Data to comply with applicable laws or as otherwise permitted by the CCPA.

11.2 Notwithstanding the foregoing, Mux is permitted to anonymize Personal Data through a reliable state of the art anonymization procedure and use such anonymized data for its own business purposes, including for research, development and security purposes, as permitted in the Agreement.

12. RETURN OR DELETION OF CUSTOMER PERSONAL DATA

Upon termination or expiry of this Agreement, Customer shall have up to ninety (90) days to submit a written request to Mux to either preserve or delete the Customer account (including all Customer Data and Personal Data in Mux's possession or control). Upon a request from Customer to delete the Customer account, Mux shall have thirty (30) days to provide confirmation of deletion. After ninety (90) days from termination of the Agreement, Customer understands and agrees that Mux may permanently delete all Customer Data including Personal Data, save that this requirement will not apply to the extent that Mux is required by Applicable Law to retain some or all of the Customer Data, or to Customer Data Mux has archived on back-up systems, which Customer Data Mux shall securely isolate and protect from any further processing, except to the extent further processing is required by Applicable Law.

13. COSTS FOR ADDITIONAL SERVICES

If Customer's and/or Customer's Customers' Instructions lead to a change from or increase of the agreed Services or in the details, scope, or security measures related to the processing of Personal Data agreed to herein and in the Agreement, Mux is entitled to charge reasonable fees for such tasks which are based on the prices agreed for rendering the Services and/or notified to Customer in advance.

14. CONTRACT PERIOD

The duration of this DPA depends on the duration of the Agreement. It commences with the initiation of the Services and shall automatically expire upon termination of all Services rendered under the Agreement with the exception of those terms that by their nature survive termination hereunder. In

such a case, the DPA shall remain applicable for such period of time as Personal Data remains in Mux's possession.

15. MODIFICATIONS

Notwithstanding anything else to the contrary in the Agreement or this DPA, Mux may modify or supplement this DPA by updating the 'Last Updated' date and posting the updated DPA to mux.com/dpa, (i) if required to do so by a supervisory authority or other government or regulatory entity, (ii) if necessary to comply with Applicable Law, (iii) when applicable, to implement amended standard contractual clauses laid down by the European Commission or respective UK or Swiss body, or (iv) to adhere to a code of conduct or certification mechanism applicable to Mux.

16. MISCELLANEOUS

16.1 If there is a conflict between the Agreement and this DPA, the terms of this DPA will prevail to the extent of the conflict. The order of precedence will be: (a) this DPA; (a) the Agreement; and (c) the Privacy Policy. To the extent they apply and there is any conflict between the SCCs and any other terms in this DPA, the Agreement, or the Privacy Policy, the provisions of the SCCs will prevail.

16.2 The parties agree that this DPA shall replace and supersede any prior data processing addendum that Mux and Customer may have previously entered into in connection with the Services.

16.3 Any claims brought in connection with this DPA will be subject to the terms and conditions, including, but not limited to, the exclusions and limitations set forth in the Agreement.

16.4 In no event does this DPA restrict or limit the rights of any data subject or of any competent supervisory authority.

16.5 Notwithstanding anything in the Agreement or any order form entered in connection therewith, the parties acknowledge and agree that Mux's access to Personal Data does not constitute part of the consideration exchanged by the parties in respect of the Agreement.

16.6 In no event shall this DPA benefit or create any right or cause of action on behalf of a third party (including a Customer's Customer), but without prejudice to the rights or remedies available to data subjects under Applicable Law or this DPA (including the DPF and SCCs).

Exhibit 1 – Details of the Processing

A. List of Parties

1. Data Exporter

The data exporter is the Customer and/or its Affiliates who are beneficiaries under the Agreement and the respective order form. Customer and Affiliate's contact person's position and contact details as well as (if appointed) the data protection officer's and (if relevant) the representative's contact details will be notified to Mux upon request. The activities relevant to the data transfer under these Clauses are: the transfer of Customer Personal Data to Mux to enable Mux to provide its Services as defined by the Agreement and the respective order form that are further described in this Exhibit 1, Section B. The data exporter is the Controller, unless it processes Personal Data of Customer's Customers, in which case the data exporter acts as a Processor.

2. Data Importer

Data Importer: Mux. Inc., 50 Beale St., 9th floor, San Francisco, CA 94105.
Data Protection Officer: Mr. Cyril Duprat, UK Site Lead – dpo@mux.com
Activities relevant to the data transferred: The processing activities are defined by the Agreement and the respective order form that are further described in Section B, below.
Role: Mux's role depends on the role of the data exporter. Mux is either a process or, if it processes Personal Data of Customer's Customer, a sub-processor.

B. Description of transfer

1. Categories of data subjects

Viewers of videos where Mux's Services have been deployed.

2. Categories of personal data transferred:

Mux Video:
Mux Video collects uploaded media and access log data of media playback requests for the purpose of utilization, performance and security validation from Content Delivery Network (CDN) partners. This may include:

- Content of the uploaded video to the extent that these contain personal data
- IP addresses;
- User Agent;
- Low Resolution geolocation data inferred from IP Address.

Mux Data:

- IP addresses (truncated);
- Browser;
- Browser version;
- Operating System;
- Operating System version;
- Autonomous System Number (ASN);

- Internet Service Provider (ISP);
- Device: version, name, model, category, brand;
- Low Resolution geolocation data inferred from IP Address.
- Metadata about the video content viewed, which includes:
    - cookie information;
    - unique identifiers;
    - details about the video content viewed;
    - Information about software or technology used to view videos;
    - Interactions with video content

3. Special categories of personal data transferred (if applicable)

N/A

4. Frequency of the transfer

The transfer is performed a continuous basis.

5. Subject matter, nature and purpose of the processing

The subject matter and nature of the processing is the use of and access to the Services by the data exporter in accordance with the Terms of Service and respective order form.

“Mux Video” processes media content (audio and video files) uploaded or streamed by customers and their end users. In this context, Mux provides an API for video hosting, encoding, and streaming services. Mux makes no attempt to extract personal information from these media files and provides the customer the ability to permanently delete the content of any uploaded file.

“Mux Data” include analytics services to help customers measure user engagement with their video content and assess the quality of playback experienced by video viewers.

6. Duration

The duration shall be as stipulated and referenced in the Agreement and the DPA.

7. Sub-processor (if applicable)

Specifics regarding the Sub-processors are set out in **Exhibit 3** hereto.

C. <u>Competent Supervisory Authority of transfer</u>

The competent supervisory authority is as outlined in the DPA.

Exhibit 2 – Technical and Organizational Security Measures

1. Access control to premises and facilities

Unauthorised access (in the physical sense) is prevented.

Technical and organizational measures to control access to premises and facilities, particularly to check authorisation:

- Access control system – RFID card for main building entrance
- Office entrance controlled during office hours and locked outside of office hours
- Building security staff
- Surveillance facilities – video cameras in hallways and building entrance

2. Access control to systems and data

Unauthorised access to IT systems is prevented.

Technical (ID/password security) and organizational (user master data) measures for user identification and authentication:

- Password procedures based upon NIST Digital Identity Guidelines (NIST SP 800-63B)
- Differentiated access rights (profiles, roles, transactions and objects)
- Logs of access
- Based on need to know

3. Disclosure control

Aspects of the disclosure of personal data are controlled.

Measures to transport, transmit and communicate or store data on data media (manual or electronic) and for subsequent checking:

- Encryption in transit and at rest
- All data access password or secure token protected

4. Job control

Commissioned data processing is carried out according to instructions.

Measures (technical/organizational) to segregate the responsibilities between the controller and processor:

- Formal commissioning via enterprise agreement or self-sign up that includes Terms of Service available online
- Monitoring of SLA, if applicable

5. Availability control

The data is protected against accidental destruction or loss.

Measures to assure data security (physical/logical):

- Backup procedures allowing for (at least) daily backups
- Data stored in highly redundant third party cloud services
- Firewall policies that only allow internal access to data
- Business continuity/Disaster recovery plan

6. Segregation control

Data collected for different purposes is processed separately.

Measures to provide for separate processing (storage, amendment, deletion, transmission) of data for different purposes:

- Microservices architecture where functions are run and administered separately

7. Security documentation

Data importer maintains a security document.

A security incident log will also be maintained which will include: incident description, date and time, reporter, recipient of

the report, effects of the incident, procedures followed to recover the data, person who recovered the data, and any data

manually re-entered.

8. Audits

Data exporter may audit data importer.

At the written request of the data exporter, data importer will provide data exporter with a confidential Report to reasonably verify compliance with the security obligations under this Annex.

9. Assistance with Data Subject Rights Requests

Data Subject Rights Requests shall be sent to gdpr@mux.com.

10. Pseudonymisation

When viewership data is collected as part of a Mux Data SDK integration, data exporter is able to choose to have the data from client SDKs sent to, and processed in, the EU only. Personal data processed in the EU is pseudonymized (specifically, viewers' IP addresses are truncated resulting in /24 addresses only) and only the pseudonymized data is sent to the United States for customer reporting and archival storage purposes.

11. Personnel security management

- Background screening
- Employment and confidentiality agreements
- Acknowledgment of acceptable uses of data and technologies

- Defined roles and responsibilities
- Security and privacy training
- Procedures for onboarding, offboarding, and changes in job duties
- Specialized training for personnel that manage third-party requests for personal data

12. ISO 27001 Certification

Data Importer holds an ISO 27001 certification.

13. Other technical and organizational security measures

- Written information security program
- Information security risk management, including regular assessments and formal risk treatments
- Regular information security program performance evaluations and continual improvement, with senior management oversight
- Logging, monitoring, and alerting for security-related events
- Strong cryptography (encryption and hashing) and key management practices to protect data both at rest and during transmission, in particular, strong encryption key management is performed (and mostly automated) using Cloud Service Provider Key Management Services (KMSs) where possible and feasible. Moreover, customer passwords are hashed before being stored in our databases, so that Mux doesn't know them
- Personal data is encrypted end-to-end on the application layer using state-of-the-art encryption methods, the encryption algorithm and its parameterization (e.g., key length, operating mode, if applicable) conform to the state-of-the-art, the strength of the encryption takes into account the specific time period during which the confidentiality of the encrypted personal data must be preserved, the encryption algorithm is implemented correctly and by properly maintained software without known vulnerabilities the conformity of which to the specification of the algorithm chosen has been verified.
- Change, configuration, and capacity management policies and procedures
- Internal policies governing transfers within the Mux group of enterprises
- Secure development processes including secure coding, application testing, and tightly controlled CI/CD procedures
- Information backup, business continuity, and disaster recovery policies and procedures
- Vulnerability management policies and procedures, including penetration testing and vulnerability scans
- Controlled orchestration of protected, immutable containers for application delivery
- Third party security management practices including third- party security and risk assessments
- Incident response policy and procedures
- Active bug bounty program to identify security flaws in Mux Data and Mux Video
- Use of password management tool

- Mobile Device Management (MDM) and endpoint technical controls including anti-malware and policy enforcement

- To the extent applicable, transparency and accountability measures that include regular publication of transparency reports relating to government requests for access to data

Ex. 3: Sub-processors

Exhibit 3 – Mux SubProcessors

	Name of sub-processor	**Mux Product**	**Country of Operation and Data processing**	**Subject matter and nature of the processing**
1	AWS	Mux Data, Mux Video	HQ: 1200 Pacific Tower 1200 12th Ave S, Seattle, Washington 98144 USA EU Data Pseudonymisation: AWS eu-central-1 region in Frankfurt (Germany - DE)	Hosting service
2	Google Cloud	Mux Video	1600 Amphitheatre Parkway, Mountain View, California 94043, USA	Hosting service
3	Cloudflare	Mux Video	101 Townsend Street, San Francisco, California 94107, USA	Content delivery network (for delivering video)
4	Fastly	Mux Video	475 Brannan Street #300, San Francisco, California 94107, USA	Content delivery network (for delivering video)
5	NS1	Mux Video	55 Broad Street, 19th Floor, New York, New York 10004, USA	Content delivery network (for delivering video)
6	Oracle	Mux Data, Mux Video	2300 Oracle Way Austin, TX 78741 USA Mux Data: EU Data Pseudonymisation	Hosting service
7	Varnish Software	Mux Video	Wallingatan 12, 111 60 Stockholm, Sweden	Content delivery network (for delivering video)
8	Castlabs	Mux Video	Wilhelmine-Gemberg-Weg 5-7, 10179 Berlin, Germany	Digital rights management

All sub-processors may have access to the Personal Data for the term of the DPA or until the service contract with the respective sub-processor is terminated or the access by the sub-processor has been excluded as agreed between Mux and Customer.

Exhibit 4 – UK and Swiss Addendum

1. UK ADDENDUM

With respect to any transfers of Personal Data falling within the scope of the UK GDPR from Customer (as data exporter) to Mux (as data importer):

1.1 neither the SCC nor the DPA shall be interpreted in a way that conflicts with rights and obligations provided for in any laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018 (together, the "**UK Data Protection Laws**");

1.2 the SCC are deemed to be amended to the extent necessary so they operate:

(a) for transfers made by Customer to Mux, to the extent that UK Data Protection Laws apply to the Customer's processing when making that transfer;

(b) to provide appropriate safeguards for the transfers in accordance with Article 46 of the UK GDPR;

1.3 the amendments referred to in Section 1.2 of this UK Addendum includes (without limitation) the following:

(a) references to "Regulation (EU) 2016/679" or "that Regulation" are replaced by "UK GDPR" and references to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article of the UK GDPR;

(b) references to Regulation (EU) 2018/1725 are removed;

(c) references to the "Union", "EU" and "EU Member State" are all replaced with the "UK";

(d) the "competent supervisory authority" shall be the Information Commissioner;

(e) clause 17 of the SCC is replaced with the following:

"*These Clauses are governed by the laws of England and Wales*";

(f) clause 18 of the SCC is replaced with the following:

"Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts";

(g) any footnotes to the SCC are deleted in their entirety.

2. SWISS ADDENDUM

This Swiss Addendum shall apply to any processing of Personal Data subject to Swiss data protection law or to both Swiss data protection law and the GDPR.

2.1 Interpretation of this Addendum

(a) Where this Addendum uses terms that are defined in the SCC as further specified in Exhibit 1 of the DPA, those terms shall have the same meaning as in the Standard Contractual Clauses. In addition, the following terms have the following meanings:

This Addendum	This Addendum to the Clauses
Clauses	The SCCs as further specified in the DPA
Swiss Data Protection Laws	The Swiss Federal Act on Data Protection of 19 June 1992 and the Swiss Ordinance to the Swiss Federal Act on Data Protection of 14 June 1993, and any new or revised version of these laws that may enter into force from time to time.

(b) This Addendum shall be read and interpreted in the light of the provisions of Swiss Data Protection Laws, and so that if fulfils the intention for it to provide the appropriate safeguards as required by Article 46 GDPR and/or Article 6(2)(a) of the Swiss Data Protection Laws, as the case may be.

(c) This Addendum shall not be interpreted in a way that conflicts with rights and obligations provided for in Swiss Data Protection Laws.

(d) Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

2.2 Hierarchy

In the event of a conflict or inconsistency between this Addendum and the provisions of the SCC or other related agreements between the Parties, existing at the time this Addendum is agreed or entered into thereafter, the provisions which provide the most protection to data subjects shall prevail.

2.3 Incorporation of the SCC

(a) In relation to any processing of personal data subject to Swiss Data Protection Laws or to both Swiss Data Protection Laws and the GDPR, this Addendum amends the DPA including the SCC as set out in Exhibit 1 of the DPA to the extent necessary so they operate:

(i) for transfers made by the data exporter to the data importer, to the extent that Swiss Data Protection Laws or Swiss Data Protection Laws and the GDPR apply to the data exporter's processing when making that transfer; and

(ii) to provide appropriate safeguards for the transfers in accordance with Article 46 of the GDPR and/or Article 6(2)(a) of the Swiss Data Protection Laws, as the case may be.

(b) To the extent that any processing of personal data is exclusively subject to Swiss Data Protection Laws, the amendments to the DPA including the SCCs as set out in Exhibit 1of the DPA and as required by Section 2.1 of this Swiss Addendum, include (without limitation):

(i) References to the "Clauses" or the "SCCs" means this Swiss Addendum as it amends the SCCs.

(ii) Clause 6 Description of the transfer(s) is replaced with:

"The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are those specified in Schedule 1 of this DPA where Swiss Data Protection Laws apply to the data exporter's processing when making that transfer."

(iii) References to "Regulation (EU) 2016/679" or "that Regulation" or "“GDPR" are replaced by "Swiss Data Protection Laws" and references to specific Article(s) of "Regulation (EU) 2016/679" or "GDPR" are replaced with the equivalent Article or Section of Swiss Data Protection Laws extent applicable.

(iv) References to Regulation (EU) 2018/1725 are removed.

(v) References to the "European Union", "Union", "EU" and "EU Member State" are all replaced with "Switzerland".

(vi) Clause 13(a) and Part C of Annex I are not used; the "competent supervisory authority" is the Federal Data Protection and Information Commissioner (the "FDPIC") insofar as the transfers are governed by Swiss Data Protection Laws;

(vii) Clause 17 is replaced to state

"These Clauses are governed by the laws of Switzerland insofar as the transfers are governed by Swiss Data Protection Laws".

(viii) Clause 18 is replaced to state:

"Any dispute arising from these Clauses relating to Swiss Data Protection Laws shall be resolved by the courts of Switzerland. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of Switzerland in which he/she has his/her habitual residence. The Parties agree to submit themselves to the jurisdiction of such courts."

2.4 To the extent that any processing of personal data is subject to both Swiss Data Protection Laws and the GDPR, the DPA including the SCCs as set out in the DPA will apply (i) as is and (ii) additionally, to the extent that a transfer is subject to Swiss Data Protection Laws, as amended by Section 2.1 and 2.3 of this Swiss Addendum, with the sole exception that Clause 17 of the SCCs shall not be replaced as stipulated under clause 2.3(b)(vii) of this Swiss Addendum.

2.5 Customer warrants that it and/or Customer Affiliates have made any notifications to the FDPIC which are required under Swiss Data Protection Laws.