Terms of Data Processing to the Mux Terms of Service Regarding the Processing of Personal Data of Customers

(hereinafter referred to as "**Mux Privacy Terms**")

PARTIES AND BACKGROUND

Mux, Inc. ("**Mux**") performs cloud-based performance analytics services to help customers measure user engagement with their video content and assess the quality of playback experienced by video viewers ("**Mux Data**"), and also provides an API for video hosting, encoding, and video streaming services ("**Mux Video**", together referred to as the "**Services**") as set out in the Terms of Service ("**Mux Terms of Service**"), further specified by the respective order form and as agreed by the customer ("**Customer**"). These Mux Privacy Terms shall be part of the Mux Terms of Service by way of this reference and constitute an integral part of the Mux Terms of Service. Capitalized terms used but not defined herein shall have the meaning given in the Mux Terms of Service.

In the course of providing the Services, Mux will process personal data (as defined below) of (i) Customer and/or (ii) Affiliates (as defined below) and/or (iii) Customer's customers located in the European Economic Area ("**EEA**"), United Kingdom ("**UK**") and/or Switzerland and/or (iii) Customer and/or Affiliate and/or Customer's customer located in other countries but whose personal data is subject to the GDPR (as defined below) (both such Customer's customer are referred to as "**Customer's Customers**") or where Customer or its Affiliates is for contractual reasons obliged to subject the data processing to data processing principles adequate to the one within the EEA, UK and/or Switzerland ("Customer Personal Data"). In the course of providing the Services, Mux may also process CCPA Personal Data (as defined below) in accordance with its obligations under the CCPA.

Customer's Customers are companies who render engage Customer as their processor and Mux as their sub-processor.

These Mux Privacy Terms regulate the data protection obligations of the Parties when processing Customer Personal Data performed under the Mux Terms of Service and will reasonably ensure such processing will only be rendered on behalf of and under the Instructions of Customer and in accordance with applicable data protection law, in particular Art. 28 et seq. GDPR, and the standard contractual clauses adopted by the European Commission as agreed in these Mux Privacy Terms.

1. DEFINITIONS

In addition to the definitions in Clause 1 and 4(a) SCC, the following definitions shall apply:

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 Mux Terms of Service or any order form based thereon.

1.2 "**Applicable Law**" means all laws, rules and regulations applicable to either party's performance under these Mux Privacy Terms, including but not limited to those applicable to the processing of

personal data. This means, in particular, the GDPR and all national laws validly amending the applicable rules for the processing of personal data, and the CCPA.

1.3 "**CCPA**" means the California Consumer Privacy Act of 2018, as amended (Cal. Civ. Code §§ 1798.100 et seq.).

1.4 "**CCPA Personal Data**" means the “Personal Information” (as defined in the CCPA) that Mux processes on behalf of Customer and/or Affiliate and/or Customer’s customers in connection with the provision of the Services.

1.5 "**GDPR**" means Regulation (EU) 2016/679 (the "**EU GDPR**") or, where applicable, the "**UK GDPR**" as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the UK European Union (Withdrawal) Act 2018 or, where applicable, the equivalent provision under Swiss data protection law;

1.6 "**Instruction**" means any documented instruction, submitted by Customer to Mux, directing Mux to perform a specific action with regard to Customer personal Data and/or CCPA Personal Data. Instructions shall initially be specified in the Mux Terms of Service and may, from time to time thereafter, be amended, supplemented or replaced by Customer by separate written or text form instructions, provided that such instructions still fall within the scope of the Services. Instruction issued for the purpose of complying with statutory claims under the GDPR such as rectification, erasure, restriction or portability of personal data fall within the scope of the Services.

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

1.8 The terms "controller", "data subject", "personal data", "personal data breach", "process", "processor", and "sub-processor”, "supervisory authority" shall have the same meaning as set out in the GDPR.

2. SCOPE

2.1 When providing the Services due under the Mux Terms of Service, Mux will process Customer Personal Data and/or CCPA Personal Data which shall be subject to the provisions contained in these Mux Privacy Terms. These Mux Privacy Terms amend the Mux Terms of Service with respect to any processing operation as described in Section 3.1 relating to Customer Personal Data and/or CCPA Personal Data provided by Customer or Customer’s Customers through Customer as amended from time to time by written agreement between the Parties.

2.2 With respect to Affiliates, by entering into the Mux Terms of Service, Customer warrants it is duly authorized:

2.2.1 to agree to these Mux Privacy Terms for and on behalf of any such Affiliates;

2.2.2 to enforce the terms of these Mux Privacy Terms including the SCC 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 these Mux Privacy Terms; and

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

2.3 Subject to Section 2.2, each Affiliate shall be bound by these Mux Privacy Terms as if it was the Customer, unless these Mux Privacy Terms differentiate between the Customer and its Affiliates, in which case the specific provision shall prevail.

2.4 The Parties agree that the EU Standard Contractual Clauses for the Transfer of Personal Data to Third Countries pursuant to European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 (*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**") as further specified in **Exhibit 1** are incorporated to these Mux Privacy Terms by reference, whereas Mux qualifies as data importer (as defined in the SCC) and Customer as data exporter (as defined in the SCC), and the following applies:

2.4.1 In the cases where the Customer acts as the controller of the Customer Personal Data it provides, the terms of the SCC Controller to Processor will apply.

2.4.2 In the case where the Customer acts as a processor for one or more of Customer's Customers, the terms of the SCC Processor to Processor will apply in relation such Customer Personal Data initially provided by Customer's Customers.

2.4.3 To the extent that the processing of Customer Personal Data is subject to UK or Swiss data protection laws, the UK Addendum and/or Swiss Addendum (as applicable) set out in **Exhibit 2** shall apply.

2.5 To the extent Mux is directly subject to the GDPR, the SCC shall be replaced with a new set of standard contractual terms once adopted by the European Commission. For this purpose, Mux will propose respective amendments to these Mux Privacy Terms which shall be deemed accepted by Customer and all its Affiliates, unless Customer objects within two (2) weeks following the receipt of the respective notice.

2.6 With regard to cases under Section 2.4.2 Customer warrants that it (i) is authorized by Customer's Customers to enter into these Mux Privacy Terms 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.

2.7 Since the Customer is the only Party which has a direct relationship with Customer's Customers, the Parties agree that

2.7.1 whenever Mux may be obligated to notify Customer's Customers under these Mux Privacy Terms including under the SCC Processor to Processor, such as under its Clause 8.6(c), Clause 9 (option 2), Clause 10(a) SCC, the Customer warrants to promptly forward such notification from Mux to the relevant Customer's Customers; and

2.7.2 any rights under these Mux Privacy Terms granted to Customer's Customer shall be exercised through Customer.

2.8 Subject to the Mux Terms of Service, additional Customer's Customers may be added by Customer to obtain the Services. In such cases, the Parties agree that Mux will process the personal data of

such additional Customer's Customers as a sub-processor under these Mux Privacy Terms including the SCC.

2.9 As explicitly allowed by Clause 2(a) s 2 of the SCC, Sections 1 through 13 of these Mux Privacy Terms are meant to supplement the SCC, in particular, by way of providing guidance for their practical implementation and are not intended to contradict, directly or indirectly, any clauses of the SCC.

2.10 In the event of any conflict between the SCC, the Mux Terms of Service or these Mux Privacy Terms, the order of prevalence between the terms included therein shall be as follows (in accordance with Clause 5 of the SCC):

(a) SCC including its Annexes,

(b) the remaining provisions of these Mux Privacy Terms, and

(c) Mux Terms of Service and other contractual documents.

3. DETAILS OF DATA PROCESSING

3.1 The details of data processing (such as subject matter, nature and purpose of the processing, categories of personal data and data subjects), as also referenced in Annex I of the Appendix to the SCC, are described in the Mux Terms of Service and in **Exhibit 3**.

3.2 For the purposes of the GDPR, when performing the Services, Mux will act either as processor or sub-processor. Mux's function as processor or sub-processor will be determined by the function of Mux's Customer. If the Customer is the controller, then Mux shall be the processor. If the Customer is the processor on behalf of its Customer's Customers, then Mux shall be the sub-processor, whereas Customer and Customer's Customers, as communicated to Mux by Customer, shall be entitled to issue Instructions under these Mux Privacy Terms.

3.3 For purposes of the CCPA, Mux will act as a "**Service Provider**" (as such term is defined in the CCPA), in its performance of its obligations pursuant to the Agreement. The following provisions apply to CCPA Personal Data:

3.3.1 **Processing of CCPA Personal Data.** Mux shall not collect, process, or retain CCPA Personal Data for any purpose other than the specific purpose of providing the Services to Customer pursuant to the Agreement, or pursuant to Customer's written instructions. Mux acknowledges and agrees that it shall not retain, use or disclose CCPA Personal Data for a commercial purpose other than providing the Services. Notwithstanding the foregoing, nothing in these Mux Privacy Terms shall restrict Mux's ability to Process CCPA Personal Data to comply with applicable laws or as otherwise permitted by the CCPA.

3.3.2 **Disclosure of CCPA Personal Data**. Mux shall not Sell, disclose, release, transfer, make **available** or otherwise communicate any CCPA Personal Data to another business or third party without the prior written consent of Customer unless and to the extent that such disclosure is made to a Subprocessor for a business purpose pursuant to Section 6. Notwithstanding the foregoing, nothing in these Mux Privacy Terms shall restrict Mux's

ability to disclose CCPA Personal Data to comply with applicable laws or as otherwise permitted by the CCPA.

3.4 Notwithstanding the foregoing, Mux is permitted to anonymize Customer Personal Data and/or CCPA 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.

4. MUX'S OBLIGATIONS

Mux's obligations are stipulated in the SCC, whereas these obligations shall be specified in accordance with Clause 2(a) s 2 of the SCC as follows:

4.1 Technical and Organizational Measures

4.1.1 In accordance with Clause 8.6(a) SCC, Mux will implement the technical and organizational measures, as also referenced in Annex II of the Appendix to the SCC, and which are described in **Exhibit 4**.

4.1.2 Without prejudice to Clause 8.6(a) SCC, if Mux significantly modifies measures specified in **Exhibit 4**, such modifications have to meet the obligations pursuant to Clause 8.6(a) SCC. Upon request, Mux shall make available to Customer a description of such modified measures which enables Customer to assess compliance with the GDPR, in particular Art. 32 GDPR, and Clause 8.6(a) SCC. Unless Customer explicitly rejects the modified measures within fourteen (14) days from receipt, the modified measures shall be deemed as accepted by Customer and Customer's Customers, whereas Customer and Customer's Customer shall not reject any modification that meets the requirements pursuant to the GDPR, in particular Art. 32 GDPR, as well as Clause 8.6(a) SCC.

4.2 Documentation and Audit Rights

4.2.1 In order to comply with its obligation to make available all information to demonstrate compliance in accordance Clauses 8.9(c) SCC, Mux shall, upon request and subject to an appropriate non-disclosure agreement, provide to Customer a comprehensive documentation of the technical and organizational measures in accordance with industry standards. The effectiveness of Mux's technical and organizational measures will be audited by an independent third-party 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.

4.2.2 Mux will allow for and contribute to audits in accordance with Clause 8.9(c) SCC Controller to Processor and Clause 8.9(d) SCC Processor to Processor, if Customer has justifiable reason to believe that Mux is not complying with these Mux Privacy Terms and, in particular, with the obligation to implement and maintain the agreed technical and organizational measures, once per year (unless there are specific indications that require

a more frequent inspection). Customer agrees to be subject to an appropriate non-disclosure agreement and in comply with Mux's policies and procedures when performing the audit. The costs associated with such audits and/or for providing additional information shall be borne by Customer, unless such audit reveals Mux's material breach with these Mux Privacy Terms.

4.2.3 In accordance with Clause 8.9(c) and (d) SCC, the aforementioned audit right can be exercised by (i) requesting additional information, (ii) accessing the databases which process Customer Personal Data or (iii) by inspecting Mux's working premises whereby in each case no access to personal data of other customers or Mux's confidential information will be granted.

4.2.4 If Customer intends to conduct an audit at Mux's premises or physical facilities, Mux will allow for such audits in accordance Clause 8.9(d) s 2 SCC Controller to Processor and Clause 8.9(f) s 2 SCC Processor to Processor, whereas Customer shall, where appropriate, give reasonable notice to Mux and agree with Mux on the time and duration of the audit and inspections shall be made during regular business hours and in such a way that business operations are not disturbed. At least one employee of Mux may accompany the auditors at any time. Mux may memorialize the results of the audit in writing which shall be confirmed by Customer.

4.2.5 In accordance with Clause 8.9(d) s 1 SCC Controller to Processor and Clause 8.9(f) s 1 SCC Processor to Processor, Customer may also engage third party auditors to perform the audit in accordance with this Section 4.2 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 such third-party auditor shall only be engaged if the auditor is bound by an appropriate non-disclosure agreement in favor of Mux prior to conducting any audit or is bound by statutory confidentiality obligations.

4.3 Notification Duties

4.3.1 Mux shall notify Customer in writing without undue delay after becoming aware of any personal data breach, and reasonably cooperate in the investigation of any such personal data breach in accordance with clause 8.6(c) SCC. However, Mux shall not make any statement or disclosure to the public, any governmental entity or any other third party about an actual or potential personal data 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.

4.3.2 In addition to the notification obligations under Clauses 8.6(c) s 2; 10(a) and 15.1(a) SCC, Mux shall inform Customer without undue delay in text form (e.g., letter, fax or e-mail) of threats to Customer Personal Data and/or CCPA Personal Data in possession of Mux by garnishment, confiscation, insolvency and settlement proceedings or other similar incidents or measures by third parties. In such case, Mux shall immediately inform the

respective responsible person/entity that Mux is not the owner of the personal data but merely the processor or sub-processor.

4.4 Data Subject Rights Requests

4.4.1 Without prejudice to Clause 10(a) SCC,

(a) Mux will promptly notify Customer of any request it has received from a data subject, who will, where appropriate, promptly notify Customer's Customer about such request.

(b) if a data subject addresses Mux with claims for access, rectification, erasure, restriction, objection or data portability, Customer hereby instructs Mux to refer the data subject to Customer, who will, where appropriate, refer data subject to Customer's Customer.

4.4.2 In the case that claims based on Art. 82 GDPR are raised against Customer, Mux shall reasonably support Customer with its defense to the extent the claim arises in connection with the processing of personal data by Mux in connection with performing the Services to Customer.

5. CUSTOMER'S OBLIGATIONS

Customer's obligations are stipulated in the SCC, whereas these obligations shall be specified in accordance with Clause 2(a) s 2 of the SCC as follows:

5.1 Customer shall provide all Instructions of its own and/or of its Customer's Customers pursuant to these Mux Privacy Terms to Mux in written, electronic or verbal form (the corresponding Clause 8.1(a) SCC Controller to Processor and Clause 8.1(b) s 1 SCC Processor to Processor shall remain unaffected). Verbal Instructions shall be confirmed immediately in written form thereafter.

5.2 Customer shall inform Mux immediately if processing by Mux might lead to a violation of data protection laws and regulations.

5.3 In the case that claims based on Art. 82 GDPR are raised against Mux, Customer shall reasonably support Mux with its defense to the extent the claim relates to the processing of Customer Personal Data by Mux in connection with performing the Services to Customer.

6. SUBPROCESSING

6.1 In accordance with Clause 9(a) SCC option 2, Mux has Customer's and/or Customer's Customers general authorization for the engagement of the sub-processor(s).

6.2 In accordance with Clause 9(b) SCC, any sub-processor is obliged to commit itself by way of written contract to comply with, in substance, the same data protection obligations as the ones under these Mux Privacy Terms.

6.3 In order to fulfil its obligation under Clause 9(a) option 2 SCC, Mux may provide a website or provide another written notice that lists all sub-processors who may have access to Customer Personal Data as well as the services they perform. In accordance with Clause 9(a) option 2 s 2 SCC, 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 Customer will immediately forward such notification to Customer's Customers, and thereby grant Customer and Customer's Customers the opportunity to object. The change in the sub-processing shall be deemed as accepted, unless Customer or Customer's Customer objects within fourteen (14) days upon notification to Customer. In the case that Customer and/or Customer's Customer, as immediately communicated by Customer to Mux, object/s to the change of sub-processors, Customer shall provide documentary evidence that reasonably shows, or reasons why the Customer or Customer's Customer reasonably believes that the sub-processor does not or cannot comply with the requirements of these Mux Privacy Terms or the SCC. Mux will use reasonable efforts to refrain from permitting such proposed sub-processor to process Customer Personal Data without adversely impacting the Services or Customer. 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.

6.4 Customer herewith agrees for itself and also on behalf of Customer's Customers, whereas Customer warrants to be duly authorized by Customer's Customers to do so, to the sub-processors as set out in **Exhibit 5**.

7. SAFEGUARDS AND SUPPORT FOR INTERNATIONAL DATA TRANSFERS

Mux undertakes to provide reasonable support to Customer to ensure compliance with the requirements imposed on the transfer of personal data to third countries with respect to data subjects located in the EEA, UK and Switzerland. In accordance with Clause 14(c) of the SCC, Mux will do so, in particular, by providing information to Customer which is reasonably necessary for Customer to complete a transfer impact assessment ("**TIA**"). Mux further agrees to implement the supplementary measures agreed upon under **Exhibit 6** in order to help Customer achieve compliance with requirements imposed on the transfer of personal data to third countries.

8. LIABILITY

In clarification of Clause 12 SCC, as regards the internal liability and without any effect as regards the external liability towards data subjects, the Parties agree that Mux's liability for breach of any terms and conditions under these Mux Privacy Terms shall be subject to the liability limitations agreed in the Mux Terms of Service. Further, no Customer Affiliate shall become beneficiary of these Mux Privacy Terms without being bound by these Mux Privacy Terms and without accepting this liability limitation. Customer will indemnify Mux against any losses that exceed the liability limitations in the Mux Terms of Service suffered by Mux in connection with any claims of Customer

Affiliates or data subjects who claim rights based on alleged violation of these Mux Privacy Terms including the SCC.

9. 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 case of Mux's compliance with its obligations pursuant to Clauses 8.6(c), (d), 8.9(a), (c), (d) or (e) and 10(b) SCC as well as in cases according to Section 4.4.2, 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.

10. CONTRACT PERIOD

The duration of these Mux Privacy Terms depends on the duration of the Mux Terms of Service. It commences with the initiation of the Services and shall automatically expire upon termination of all Services rendered under the Mux Terms of Service, unless where processing of Customer Personal Data continues beyond the term of the Services under the Mux Terms of Service according to these Mux Privacy Terms. In such a case, these Mux Privacy Terms shall remain applicable for such a period of time.

11. MODIFICATIONS

Mux may modify or supplement these Mux Privacy Terms with two (2) weeks prior notice to Customer, (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) to implement amended standard contractual clauses laid down by the European Commission or a respective UK or Swiss body (iv) to adhere to a code of conduct or certification mechanism approved or certified pursuant to Art. 40, 42 and 43 of the GDPR. Customer shall notify Mux if it does not agree to a modification, in which case Mux may terminate these Mux Privacy Terms and the Mux Terms of Service with two (2) weeks' prior written notice, whereby in the case of an objection not based on non-compliance of the modifications with applicable data protection law, Mux shall remain entitled to claim its agreed remuneration until the end of the term that had been agreed by the Parties.

12. CHOICE OF LAW AND PLACE OF JURISDICTION

These Mux Privacy Terms is governed by, and shall be interpreted in accordance with, the law that is stipulated by the Parties in **Exhibit 3,** whereas the place of jurisdiction is specified in **Exhibit 3**.

13. MISCELLANEOUS

In the event a clause under the Mux Terms of Service has been found to violate the GDPR or any other Applicable Law, the Parties will mutually agree on modifications to the Mux Terms of Service to the extent necessary to comply with Applicable Law.

Exhibit 1 – Specifications Regarding the Standard Contractual Clauses for International Data Transfers

Standard Contractual Clauses

1. Clause 2.4.1 sets out the cases where Module Two applies, clause 2.4.2 sets out the cases where Module Three applies.
2. Clause 7 of the Standard Contractual Clauses (Docking Clause) does not apply.
3. Clause 9(a) option 2 (General written authorization) is selected, and the time period to be specified is determined in clause 6.3 of the Mux Privacy Terms.
4. The option in Clause 11(a) of the Standard Contractual Clauses (Independent dispute resolution body) does not apply.
5. With regard to Clause 17 of the Standard Contractual Clauses (Governing law), the Parties agree that, option 1 shall apply and the governing law shall be the law of the Republic of Ireland.
6. In Clause 18 of the Standard Contractual Clauses (Choice of forum and jurisdiction), the Parties submit themselves to the jurisdiction of the courts of the Republic of Ireland.
7. For the Purpose of Annex I of the Standard Contractual Clauses, Exhibit 3 to the Mux Privacy Terms contains the specifications regarding the parties, the description of transfer, and the competent supervisory authority.
8. For the Purpose of Annex II of the Standard Contractual Clauses, Annex 4 to this Exhibit 1 to the Mux Privacy Terms contains the technical and organizational measures.
9. Annex III of the Standard Contractual Clauses Annex III does not apply as option 2 of Clause 9(a) applies.

Exhibit 2 – UK and Swiss Addendum

1. UK ADDENDUM

With respect to any transfers of Customer 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 Mux Privacy Terms 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

As stipulated in Section 2.4.3 of the Mux Privacy Terms, this Swiss Addendum shall apply to any processing of Customer 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 Mux Privacy Terms, 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 SCC as further specified in in Exhibit 1
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 Mux Privacy Terms including the SCC as further specified in Exhibit 1 of the Mux Privacy Terms 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 Mux Privacy Terms including the SCCs as further

specified in Exhibit 1of the Mux Privacy Terms 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 these Mux Privacy Terms 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."

Until the entry into force of the revised Swiss Data Protection Laws, the SCC shall also protect personal data of legal entities and legal entities shall receive the same protection under the SCC as natural persons.

2.4 To the extent that any processing of personal data is subject to both Swiss Data Protection Laws and the GDPR, the Mux Privacy Terms including the SCC as further specified in Exhibit 1 of the Mux Privacy Terms 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.

Exhibit 3 – Specifications of the Processing

A. List of Parties

1. Data Exporter

The data exporter is the Customer and/or its Affiliates who are (i) either located in the European Economic Area ("EEA") or (ii) are located in other countries but are subject to the GDPR or (iii) are for contractual reasons obliged to subject the data processing to data processing principles adequate to the one within the EEA and are beneficiaries under the Mux Terms of Service 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 Mux Terms of Service and the respective order form that are further described in this Exhibit 3, Section B. The data exporter is the controller, unless it processes Customer Personal Data of Customer's Customer in accordance with clause 2.4.2 of the Mux Privacy Terms, in which case the data exporter acts as a processor.

2. Data Importer

Data Importer: Mux. Inc., 1182 Market St. Suite 425 San Francisco, CA 94102.
Contact person: Mrs. Becca Axvig – becca@mux.com, Head of People.
Data Protection Officer: Mrs. Becca Axvig – becca@mux.com, Head of People
EU Representative: Mr. Cyril Duprat – cyril@mux.com, EMEA Revenue Manager & UK Site Lead
UK Representative: Mr. Cyril Duprat – cyril@mux.com, EMEA Revenue Manager & UK Site Lead
Activities relevant to the data transferred: The processing activities are defined by the Mux Terms of Service and the respective order form that are further described in under Exhibit 3, Section B.
Role: Mux's role depends on the role of the data exporter. Mux is either a process or, if it processes Customer 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 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 – see Exhibit 4.10);
- Browser;
- Browser version;
- Operating System;
- Operating System version;
- Autonomous System Number (ASN);
- Internet Service Provider (ISP);
- Device Information;
- Geolocation (country, region, and in some cases, city, latitude and longitude). All latitude/longitude numbers are restricted to only 1 decimal point of accuracy.
- 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 Section 10 of the Mux Privacy Terms.

7. Sub-processor (if applicable)

Specifics regarding the Sub-processors are set out in Exhibit 5.

C. Competent Supervisory Authority of transfer

Where the data exporter is established in an EU Member State: The supervisory authority of the country in which the data exporter established is the competent authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of the GDPR in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of the GDPR: The competent supervisory authority is the one of the Member State in which the representative is established.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of the GDPR in accordance with its Article 3(2) without, however, having to appoint a representative pursuant to Article 27(2) of the GDPR: The competent supervisory authority is the supervisory authority in Ireland, namely the Data Protection Commission (https://www.dataprotection.ie/).

Exhibit 4 – Technical and Organizational 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 (incl. special characters, minimum length, change of password, and two factor authentication where possible)
- Raw data guarded by VPN access
- Differentiated access rights (profiles, roles, transactions and objects)
- Logs of VPN access

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/tunneling (VPN = Virtual Private Network)
- All data delivered over encrypted HTTPS
- 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

- 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

12. ISO 27001 Certification

Data Importer aims to achieve ISO 27001 certification by December 31, 2021.

13. Other technical and organizational security measures

- 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, 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
- Change, configuration, and capacity management policies and procedures
- 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

Exhibit 5 – List of Sub-processors

Please complete the following list as to the sub-processors which are utilized by Mux at the commencement of the processing, or declare "None" if not applicable:

	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 location: 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)

All sub-processors may have access to the Customer Personal Data for the term of the Mux Privacy Terms 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 6 - Supplementary Measures for International Data Transfers

Mux commits to implementing the following supplementary measures based on guidance provided by EU supervisory authorities[1] in order to enhance the protection for Customer Personal Data in relation to the processing in a third country.

1. Additional Technical Measures

1.1 Encryption

1.1.1 The personal data is transmitted (between the Parties and by Processor between data centers as well as to a sub-processor and back) using strong encryption.

Hereby, it is ensured that the encryption protocols employed are state-of-the-art and provide effective protection against active and passive attacks with resources known to be available to the public authorities of this third country, the parties involved in the communication agree on a trustworthy public-key certification authority or infrastructure, specific protective and state-of-the-art measures are used against active and passive attacks on the sending and receiving systems providing transport encryption, including tests for software vulnerabilities and possible backdoors, in case the transport encryption does not provide appropriate security by itself due to experience with vulnerabilities of the infrastructure or the software used, personal data is also 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 and can be considered robust against cryptanalysis performed by the public authorities when data is transiting to this third country taking into account the resources and technical capabilities (e.g., computing power for brute-force attacks) available to them[2], 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, e.g., by certification, the keys are reliably managed (generated, administered, stored, if relevant, linked to the identity of the intended recipient, and revoked), by Customer or by an entity trusted by Customer under a jurisdiction offering an essentially equivalent level of protection.

1.1.2 The personal data at rest is stored by Processor using strong encryption.

[1] EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, V 2.0, 18 June 2021, Annex 2.

[2] For the assessment of the strength of encryption algorithms, their conformity with the state-of-the-art, and their robustness against cryptanalysis over time, Customer can rely on technical guidance published by official cybersecurity authorities of the EU and its member states. See e.g. ENISA Report « What is "state of the art" in IT security? », 2019, https://www.enisa.europa.eu/news/enisa-news/what-is-state-of-the-art-in-it-security; guidance given by the German Federal Office for Information Security in its Technical Guidelines of the TR-02102 series and "Algorithms, Key Size and Protocols Report (2018), H2020-ICT-2014 – Project 645421, D5.4, ECRYPT-CSA, 02/2018" at https://www.ecrypt.eu.org/csa/documents/D5.4-FinalAlgKeySizeProt.pdf.

The encryption algorithm and its parameterization (e.g., key length, operating mode, if applicable) conform to the state-of-the-art and can be considered robust against cryptanalysis performed by the public authorities in the recipient country taking into account the resources and technical capabilities (e.g., computing power for brute-force attacks) available to them[5]*. The strength of the encryption and key length* 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, e.g., by certification. The keys are reliably managed (generated, administered, stored, if relevant, linked to the identity of an intended recipient, and revoked).*

2. Additional Organizational Measures

2.1 Internal policies for governance of transfers especially with groups of enterprises

2.1.1 Adoption of adequate internal policies with clear allocation of responsibilities for data transfers, reporting channels and *standard* operating procedures for cases of formal or informal requests from public authorities to access the data.

Especially in case of transfers among groups of enterprises, these policies may include, among others, the appointment of a specific team, composed of experts on IT, data protection and privacy laws, to deal with requests that involve personal data transferred from the EEA; the notification to the senior legal and corporate management and to Customer upon receipt of such requests; the procedural steps to challenge disproportionate or unlawful requests and the provision of transparent information to data subjects.

2.1.2 Development of specific *training* procedures for personnel in charge of managing requests for access to personal data from public authorities, which should be periodically updated to reflect new legislative and jurisprudential developments in the third country and in the EEA.

The training procedures should include the requirements of EU law as to access by public authorities to personal data, in particular as following from Article 52(1) of the Charter of Fundamental Rights. Awareness of personnel should *be raised in particular by means of assessment of practical examples of public authorities' data access requests and by applying the standard following from Article 52(1) of the Charter of Fundamental Rights to such practical examples. Such training should take into account the particular situation of the Processor, e.g. legislation and regulations of the third country to which Processor is subject to, and should be developed where possible in cooperation with Customer.*

2.2 Transparency and accountability measures

Regular publication of transparency reports or summaries regarding governmental requests for access to data and the kind of reply provided, insofar publication is allowed by local law.

2.3 **Organizational methods and data minimization measures**

2.3.1 Already existing organizational requirements under the accountability principle, such as the adoption of strict and granular data access and confidentiality policies and best practices, based on a strict need-to-know principle, monitored with regular audits and enforced through disciplinary measures. Data minimization should be considered in this regard, in order to limit the exposure of personal data to unauthorized access. For example, in some cases it might not be necessary to transfer certain data (e.g. in case of remote access to EEA data, such as in support cases, when restricted access is granted instead of full access; or when the provision of a service only requires the transfer of a limited set of data, and not an entire database). In the case at hand, the Parties will implement this as follows: confidentiality obligations of personnel; acknowledgment of acceptable uses of data and technologies; defined roles and responsibilities; security and privacy training; and procedures for onboarding, offboarding, and changes in job duties

2.3.2 Development and implementation of best practices by both Parties to appropriately and timely involve and provide access of information to their respective data protection officers, if existent, and to their legal and internal auditing services on matters related to international transfers of personal data transfers.

2.4 **Others**

Adoption and regular review by Processor of internal policies to assess the suitability of the implemented complementary measures and identify and implement additional or alternative solutions when necessary, to ensure that an essentially equivalent level of protection to that guaranteed within the EEA of the personal data transferred is maintained.

3. Additional Contractual Measures

3.1 **Transparency obligations**

3.1.1 Processer declares that (1) it has not purposefully created back doors or similar programming that could be used to access the system and/or personal data, (2) it has not purposefully created or changed its business processes in a manner that facilitates access to personal data or systems, and (3) that national law or government policy does not require Processor to create or maintain back doors or to facilitate access to personal data or systems or for Processor to be in possession or to hand over the encryption key.

3.1.2 Processor will verify the validity of the information provided for the TIA questionnaire on a regular basis and provide notice to Customer in case of any changes without delay. Clause 14(e) SCC shall remain unaffected.

3.2 **Obligations to take specific actions**

In case of any order to disclose or to grant access to the personal data, Processor commits to inform the requesting public authority of the incompatibility of the order with the safeguards contained in the Article 46 GDPR transfer tool and the resulting conflict of obligations for Processor.

3.3 Empowering data subjects to exercise their rights

Processor commits to fairly compensate the data subject for any material and non-material damage suffered because of the disclosure of his/her personal data transferred under the chosen transfer tool in violation of the commitments it contains.

Notwithstanding the foregoing, Mux shall have no obligation to indemnify the data subject to the extent the data subject has already received compensation for the same damage.

Compensation is limited to material and non-material damages as provided in the GDPR and excludes consequential damages and all other damages not resulting from Mux´s infringement of the GDPR.