DATA PROCESSING ADDENDUM

1. BACKGROUND

1.1 This Data Processing Addendum ("**DPA**") forms a part of the Enterprise Software License Terms and Conditions ("**Terms**") to which it is attached.

1.2 In the event of a conflict between any of the provisions of this DPA and the Terms, the provisions of this DPA shall prevail.

2. DEFINITIONS

2.1 Unless otherwise set out below, each capitalised term in this DPA shall have the meaning set out in the Agreement and the following capitalised terms used in this DPA shall be defined as follows:

(a) "**CCPA**" means the California Consumer Privacy Act of 2018 and any regulations promulgated thereunder, in each case, as amended from time to time;

(b) "**Customer Personal Data**" means (a) the personal data described in Part 1 of ANNEX 2 and any other personal data made available to Mux in connection with Mux's provision of the Services, and (b) any other information made available to Mux in connection with the Services that constitutes "personal information" as defined in the CCPA;

(c) "**Data Protection Laws**" means all laws and regulations of any jurisdiction applicable to the Processing of Customer Personal Data under the Agreement, including the GDPR, the CCPA, and all other laws and regulations relating to privacy, direct marketing or data protection;

(d) "**European Economic Area**" or "**EEA**" means the Member States of the European Union together with Iceland, Norway, and Liechtenstein;

(e) "**GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation);

(f) "**Party**" means either the Customer and/or Mux;

(g) "**Security Incident**" means any personal data breach (as defined in GDPR) or other incident that has resulted in any accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, any Customer Personal Data;

(h) "**Standard Contractual Clauses**" means the Standard Contractual Clauses (processors) approved by European Commission Decision C(2010)593 set out in ANNEX 1 to this DPA or any subsequent version thereof released by the European Commission (which will automatically apply), and which includes Part 1 of ANNEX 2 (Details of the Transfer) and ANNEX 3 (Technical and Organizational Measures) to this DPA;

(i) "**Subprocessor**" means any Processor engaged by Mux that will process Customer Personal Data; and

(j) the terms "**personal data**", "**Controller**", "**Processor**", "**Data Subject**", "**Process**" and "**Supervisory Authority**" shall have the same meaning as set out in the GDPR.

3. DATA PROCESSING

3.1 **Instructions for Data Processing.** Mux will only Process Customer Personal Data in accordance with (a) the Agreement, to the extent necessary to provide the Services to the Customer; (b) the Customer's written instructions, unless Processing is required by European Union or Member State law to which Mux is subject, in which case Mux shall, to the extent permitted by applicable law, inform the Customer of that legal requirement before Processing that

Customer Personal Data; and (c) its obligations under Data Protection Laws. Mux shall not perform the Services in a manner that causes Customer to violate Data Protection Laws, and Mux shall notify Customer in writing immediately if, in Mux's reasonable opinion, Mux believes that any instruction given by Customer infringes Data Protection Laws.

3.2 Processing outside the scope of this DPA or the Agreement will require prior written agreement between the Customer and Mux on additional instructions for Processing.

4. TRANSFER OF PERSONAL DATA

4.1 Mux shall not permit, allow or otherwise facilitate Subprocessors to Process Customer Personal Data without the prior written consent of Customer and unless Mux enters into a written agreement with the Subprocessor which imposes the same obligations on the Subprocessor with regard to their Processing of Customer Personal Data as are imposed on Mux under this DPA. Upon request, Mux shall provide Customer with a current list of the names and contract information of any Subprocessors (the "**Subprocessor List**"). Mux shall provide sixty (60) days' prior notice by email to Customer of any addition of a new Subprocessor to the Subprocessor List. If Customer objects in writing to Mux's proposed use of a new Subprocessor, Mux will use reasonable efforts to refrain from permitting such proposed Subprocessor 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 written objection. Upon receipt of such notice, Customer may terminate the Agreement 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.

4.2 **Liability of Subprocessors**. Mux shall at all times remain responsible for compliance with its obligations under the DPA and will be liable to the Customer for the acts and omissions of any Subprocessor approved by the Customer as if they were the acts and omissions of Mux.

4.3 **International Transfers of Personal Data**. To the extent that the Processing of Customer Personal Data by Mux involves the export of such Personal Data to a country or territory outside the EEA, other than a country or territory ensuring an adequate level of protection for the rights and freedoms of Data Subjects in relation to the Processing of Personal Data as determined by the European Commission (an "**International Transfer**"), such International Transfer shall be governed by the Standard Contractual Clauses. In the event of any conflict between any terms in the Standard Contractual Clauses, this DPA and the Agreement, the Standard Contractual Clauses shall prevail. The Parties agree to amend the Standard Contractual Clauses if required in accordance with a relevant European Commission decision or Data Protection Laws.

5. DATA SECURITY, AUDITS AND SECURITY NOTIFICATIONS

5.1 **Mux Security Obligations**. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Mux shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including, where applicable by virtue of Article 28(3)(c) of the GDPR, and as appropriate, the measures referred to in Article 32(1) of the GDPR. Without limiting the generality of the foregoing, Mux shall put in place and maintain the technical and organisational measures set out in ANNEX 3.

5.2 **Service Provider Audits**. The Customer may audit (by itself or using independent third party auditors) Mux's compliance with this DPA (including the technical and organisational measures as set out in ANNEX 3), including by conducting audits of Mux's (and Subprocessors') data processing facilities and such audits may be performed at least once annually.

5.3 Where applicable by virtue of Article 28(3)(h) of the GDPR, Mux shall make available to the Customer on request all information necessary to demonstrate compliance with this DPA. Mux shall immediately inform the Customer if, in its opinion, an instruction pursuant to this clause 5.3 infringes applicable Data Protection Laws.

5.4 **Security Incident Notification.** If Mux or any Subprocessor becomes aware of, or has reason to suspect that there has been, a Security Incident, Mux will (a) notify the Customer of the Security Incident without undue delay but in any event no later than 72 hours thereafter, (b) investigate the Security Incident and provide such reasonable assistance to the Customer (and any law enforcement or regulatory official) as required by Customer to investigate and remediate the Security Incident, and (c) remedy any non-compliance with this DPA. Without limiting the generality of the foregoing, Mux shall promptly provide Customer with the following information as it becomes available:

(a) a detailed description of the nature of the Security Incident, including where possible the categories and approximate number of Data Subjects and Customer Personal Data records concerned;

(b) a description of the measures taken or proposed to be taken to address the Security Incident, including, where appropriate, measures to mitigate its possible adverse effects; and

(c) whether any regulatory authority, the Data Subjects or the media have been informed or are otherwise already aware of the Security Incident, and their response.

Customer may require that Mux's access to, or Processing or storing of Customer Personal Data be suspended, connectivity with Customer be terminated, or other appropriate action be taken pending such resolution. Additionally, Mux agrees to keep Customer informed of progress and actions taken to address the Security Incident and prevention of future such Security Incidents, and to provide Customer with all facts about the Security Incident as appropriate for Customer to conduct its own assessment of the risk to Customer Personal Data and of Customer's overall exposure to such Security Incident. Except as required by applicable law or with Customer's prior written consent, Mux shall not make any statement or disclosure to the public, any governmental entity or any other third party about an actual or potential Security Incident that references Customer or from which Customer's involvement could be reasonably inferred.

If and solely to the extent the Security Incident was the result of the actions or omissions of Mux or its Subprocessors, Mux shall be responsible for the cost and expense of notification (including notification to governmental entities and affected Individuals), credit monitoring and remediation activities solely to the extent (a) required by the Agreement, (b) Customer, Mux or its Subprocessors are required to perform such activities under applicable laws or (c) required in connection with Customer's exercise of its rights or remedies at law or under the Agreement in respect of any Security Incident. Mux agrees to reasonable co-operation with Customer and to take such reasonable commercial steps as are directed by Customer to assist in the investigation, mitigation and remediation of the Security Incident in the relevant jurisdictions.

5.5 **Mux Employees and Personnel.** Mux shall treat the Customer Personal Data as the Confidential Information of the Customer, and shall ensure that:

(a) access to Customer Personal Data is limited to those employees or other personnel who have a business need to have access to such Customer Personal Data; and

(b) any employees or other personnel have agreed in writing to protect the confidentiality and security of Customer Personal Data.

6. ACCESS REQUESTS AND DATA SUBJECT RIGHTS

6.1 **Data Subject Requests**. Except as required (or where prohibited) under applicable law, Mux shall notify the Customer of any request received by Mux or any Subprocessor from a Data Subject in respect of their personal data included in the Customer Personal Data, and shall not respond to the Data Subject without Customer's prior written instructions.

6.2 Mux shall promptly assist the Customer with ensuring its obligations to clients or under applicable Data Protection Laws in respect of such requests or complaints, including, without limitation, meeting any deadlines imposed by such obligations. Without limited the generality of the foregoing, Mux shall:

(a) provide the Customer with the ability to correct, delete, block, access or copy the personal data of a Data Subject, or

(b) promptly correct, delete, block, access or copy Customer Personal Data within the Services at the Customer's request.

6.3 **Government Disclosure.** Mux shall promptly notify the Customer of any inquiry or request relating to Customer Personal Data by a governmental or regulatory body or law enforcement authority (including any data protection supervisory authority) (collectively, a "**Regulator**") unless otherwise prohibited by law or a legally binding order of such Regulator. If Mux or Customer receives such an enquiry or request from a Regulator, Mux shall promptly and without undue delay provide Customer with such information as Customer may reasonably request to satisfy such inquiry or request. Unless Customer notifies Mux that Mux will be responsible for handling a particular communication or correspondence with a Regulator or a Regulator requests in writing to engage directly with Mux, Customer will handle all communications and correspondence relating to Customer Personal Data or the Services.

7. ASSISTANCE

7.1 Mux shall provide the Customer with any information or assistance reasonably requested by the Customer for the purpose of complying with any of the Customer's obligations under applicable Data Protection Laws, including:

(a) where applicable by virtue of Article 28(3)(e) of the GDPR, taking into account the nature of the Processing, assisting the Customer by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests for exercising Data Subject rights laid down in the GDPR; and

(b) where applicable by virtue of Article 28(3)(f) of the GDPR, providing reasonable assistance to the Customer with any data protection impact assessments which are referred to in Article 35 of GDPR and with any prior consultations to any Supervisory Authority of the Customer which are referred to in Article 36 of GDPR, in each case solely in relation to Processing of the Customer Personal Data and taking into account the nature of the Processing and information available to Mux.

8. CALIFORNIA REQUIREMENTS

8.1 The Parties agree that for purposes of this section 8, "**Services**" shall mean Mux's performance of its obligations and exercise of its rights under the Agreement and this Section 8 applies only to Customer Personal Data that constitutes personal information as defined in and subject to the CCPA.

8.2 Subject to section 8.3, Mux shall not retain, use, or disclose Customer Personal Data for any purpose other than for the specific purpose of performing the Services.

8.3 Mux shall not (i) sell any Customer Personal Data; (ii) retain, use or disclose any Customer Personal Data for any purpose other than for the specific purpose of performing the Services, including retaining, using, or disclosing the Customer Personal Datafor a commercial purpose (as defined in the CCPA) other than provision of the Services; or (iii) retain, use or disclose the Customer Personal Data outside of the direct business relationship Mux and Customer. Mux hereby certifies that it understands its obligations under this section 8.3 and will comply with them.

8.4 Notwithstanding anything in the Agreement to the contrary, any reference in this Agreement to (a) "aggregate" or "aggregated" information means information that constitutes "aggregate consumer information" under the CCPA and (b) "anonymous" or "anonymized" information means information that has been "deidentified" as defined by the

CCPA and with respect to which Mux has met the same requirements that a business Is required to meet under California Civil Code Section 1798.140(h).

8.5 This Section 8 shall not be construed to limit any other requirement or obligation under this DPA.

9. INDEMNITY; LIMITATIONS ON LIABILITY

9.1 **Indemnity.** Mux shall indemnify, defend and hold harmless the Customer and its officers, directors, employees, agents, affiliates, successors and permitted assigns (each an "**Indemnified Party**", and collectively the "**Indemnified Parties**") against any and all losses, damages, liabilities, deficiencies, claims, actions, judgments, settlements, interest, awards, penalties, fines, costs, or expenses of whatever kind, including legal fees and court fees, (collectively, "**Losses**") arising out of any breach of this DPA, including, without limitation, Losses arising out of a Security Incident resulting from such breach, except where such Losses result from an Indemnified Party's gross negligence, willful misconduct, or recklessness. This indemnity obligation shall not be subject to any exclusion or limitation of liability provisions in the Agreement.

10. DURATION AND TERMINATION

10.1 **Deletion of data**. On termination of this Agreement for any reason or upon Customer's request, Mux will cease Processing Customer Personal Data, return a copy of the Customer Personal Data to Customer and then securely delete or destroy, as applicable, all Customer Personal Data in Mux's possession (except as prohibited by law or other explicit data retention and/or return provisions in this Agreement).

ANNEX 1

STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

For the purposes of this ANNEX 1, references to the "data exporter" shall be to the Customer and references to the "data importer" shall be to Mux (each a "*party*"; together "*the parties*").

Clause 1

Definitions

For the purposes of the Clauses:

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

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

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

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

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

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

Clause 2

Details of the transfer

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

Clause 3

Third-party beneficiary clause

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

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

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

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

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

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

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

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

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

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

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

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

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

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

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

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

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

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

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

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

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

  (ii) any accidental or unauthorised access, and

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

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

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

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial

information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

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

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

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

Clause 6

Liability

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

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

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

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

Clause 7

Mediation and jurisdiction

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

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

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

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

Clause 8

Cooperation with supervisory authorities

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

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

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

Clause 9

Governing Law

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

Clause 10

Variation of the contract

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

Clause 11

Subprocessing

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

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

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

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

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

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

ANNEX 2

PART 1

Details of the transfer forming part of the Standard Contractual Clauses

Data exporter

The data exporter is the Customer

Data importer

The data importer is Mux

Data subjects

The personal data transferred concern the following categories of data subjects:

- Viewers of videos where Mux Data has been deployed

Categories of data

The personal data transferred concern the following categories of data:

- All categories of Customer Personal Data, including, without limitation, such Customer Personal Data listed at https://docs.mux.com/docs/metadata.

Processing operations

The personal data transferred will be subject to the following basic processing activities: transmitting, collecting, storing and analyzing data in order to provide the Services to the Customer, and any other activities related to the provision of the Services or specified in the Agreement.

PART 2

Details of the Processing of Customer Personal Data

This Part 2 of ANNEX 2 includes certain details of the processing of Customer Personal Data as required by Article 28(3) of the GDPR.

Subject matter and duration of the Processing of Customer Personal Data

The subject matter of the Processing of Customer Personal Data is the use of and access to the Services by the Customer in accordance with the Agreement.

The duration of the Processing of Customer Personal Data is the later of the Term of the Data Processing Addendum or Mux's deletion of Customer Personal Data in its possession, custody or control (including Customer Personal Data in the possession, custody or control of Suprocessors).

The nature and purpose of the Processing of Customer Personal Data

The Processing of Customer Personal Data provided by Customer to Mux for the purposes of providing the Services to the Customer.

The types of Customer Personal Data to be processed

- IP addresses;
- 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.
- Information about data subjects who view video content including;
    - cookie information;
    - unique identifiers;
    - details about the video content viewed;
    - Information about software or technology used to view videos;
    - Interactions with video content

The categories of data subject to whom the Customer Personal Data relates

- Viewers of videos whose personal data Mux Processes in its provision of the Services.

The obligations and rights of the Customer

The obligations and rights of the Customer are as set out in this DPA and the Agreement.

ANNEX 3

TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

1. Access control to premises and facilities
Unauthorized access (in the physical sense) is prevented.
Technical and organizational measures to control access to premises and facilities, particularly to check authorization:

- 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
Unauthorized 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.