



## MK.IO DATA PROCESSING AGREEMENT

BETWEEN (1) MK Systems USA Inc. having its principal place of business at 2611 Internet Blvd, Ste 120, Frisco, Texas 75034 USA for and on behalf of itself and its Affiliates (“Supplier”), and (2) you (“You”), each a “Party” and together the “Parties”.

This MK.IO Data Processing Agreement (“DPA”) is incorporated into and made a part of the License Agreement – MK.IO Video Services (including any applicable Service Specific Terms) in effect between Supplier and You (the “License Agreement”). If any provisions of this DPA and the License Agreement conflict, including any previously executed or incorporated data processing agreement or privacy terms, then the provisions of this DPA shall control. Except for any changes made by this DPA, the License Agreement remains unchanged and in full force and effect.

BY SUBSCRIBING TO THE SERVICES (INCLUDING WHERE APPLICABLE BY SELECTING “GET IT NOW”, “ACTIVATE”, “SUBSCRIBE” OR “CLICK TO BUY”), OR BY ACCESSING OR USING A SERVICE, OR BY DOWNLOADING, INSTALLING, COPYING, OR USING ANY ASSOCIATED SOFTWARE PROVIDED BY SUPPLIER IN CONNECTION WITH A SERVICE, YOU ACKNOWLEDGE AND AGREE: (1) THAT YOU HAVE READ AND UNDERSTAND THIS DPA; (2) THAT YOU AGREE TO BE BOUND BY EACH AND EVERY TERM OF THIS DPA WHEN ACCESSING AND USING A SERVICE; AND (3) IF YOU ARE ENTERING INTO THIS DPA ON BEHALF OF A COMPANY, THAT YOU HAVE THE POWER AND AUTHORITY TO DO SO AND TO BIND SUCH COMPANY.

IF YOU DO NOT AGREE TO ANY OF THE TERMS AND CONDITIONS OF THIS DPA, YOU MAY NOT USE THE SERVICES (OR ASSOCIATED SOFTWARE) PROVIDED BY SUPPLIER.

### BACKGROUND

- (A) You are subscribing to Services that enable the encoding (and distribution, including where applicable packaging, encryption, and streaming) of Content in the cloud, and in providing such Services to You it may be necessary for Supplier and/or its Affiliates to Process certain Personal Data on Your behalf.
- (B) When setting up Your MK.IO subscription the Supplier will collect and Process limited Personal Data from You for the purpose of managing and administering Your account and/or configuring the Services. When providing the Services, Supplier does not collect Personal Data, but may Process Personal Data embedded within the Content You choose to encode (and distribute where applicable). You determine what Personal Data is collected, what data elements are embedded within the Content, as well as the location(s) at which the Processing of such Personal Data takes place, and other encoding parameters. Supplier has no control over and no (or limited, e.g. if providing transcribing or subtitle functionality) visibility into the specific data elements of the Personal Data embedded within Content; and all such control and visibility is determined by You.
- (C) The Supplier and its Affiliates are committed to respecting everyone’s privacy through the lawful and proper handling of Personal Data to which they have access, including that of employees, contingent workforce, partners, customers, and end-users (including Your subscribers). Suppliers to the

Supplier and its Affiliates are held to the same level of commitment when it comes to privacy.

- (D) The terms and conditions specified herein shall apply if and when Supplier and/or its Affiliates Process Personal Data on Your behalf, details of the Personal Data and proposed Processing activities being as described in the Appendix to this DPA.

### AGREED TERMS

#### I Definitions

I.1 For the purposes of this DPA, the following words and expressions shall have the meaning assigned to them below unless the context would obviously require otherwise:

“Affiliate” means (i) for Supplier, any entity that controls, is controlled by, or under common control with, MK Systems USA Inc.; or (b) for You, any entity that is directly or indirectly controlled or under common control with You;

“Applicable Privacy Laws” means all laws and regulations applicable to the Processing of Personal Data under this DPA (including *where applicable* and without limitation the California Consumer Privacy Act 2018 (“CCPA”), Swiss Data Protection laws, the UK Data Protection Act 2018, and the EU General Data Protection Regulation (2016/679) (“EU GDPR”), the laws of a relevant EU member state, and any supplemental or

	successor laws in any other relevant jurisdiction);		
“Content”	means any text, graphics, video, images, audio or any other media, information, material or content (including metadata and any relevant Personal Data) that You choose to provide to Supplier in connection with Your use of the Services (including files sent for encoding and distribution);	“Processing”	shall mean any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction, as defined in the Applicable Privacy Laws (and “Process”, “Processed” etc. shall be construed accordingly);
“Controller”	means the legal entity which, alone, on behalf of others, or jointly with others, determines the purposes and means of the Processing of Personal Data;	“Processor”	means the legal entity that Processes the Personal Data on behalf of the Controller;
“Data Subject”	means an identifiable natural person, who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;	“SCCs, or Standard Contractual Clauses”	means the current approved standard contractual clauses (or such other instrument(s) approved by the European Commission that will replace or succeed such clauses) for the transfer of Personal Data to Processors established in third countries outside the EEA in which the data protection regime is regarded as inadequate;
“DPA”	means this data processing agreement, including any and all subsequent amendments thereto, and comprising the terms and conditions in the main body of this document, together with the schedules, appendices, annexes and any attachments, and any documents expressly incorporated by reference;	“Services”	shall have the meaning given to it in the License Agreement;
“European Economic Area or EEA”	means the economic territory formed by member states of the European Union (“EU”) and countries that are members of the European Free Trade Association (excluding Switzerland);	“UK Addendum”	means the current approved international data transfer addendum (or such other instrument approved by the UK government that will replace or succeed such addendum) for the transfer of Personal Data to Processors established in third countries outside the UK in which the data protection regime is regarded as inadequate.
“Personal Data Breach”	shall mean any breach of security or privacy leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, the Personal Data transmitted, stored or otherwise Processed by Supplier hereunder;		
“Personal Data”	shall mean that information set out in Annex I of this DPA;		
“Privacy Authority”	means an independent regulatory or supervisory public authority with responsibility for privacy or data protection matters in a relevant jurisdiction;		

1.2 Capitalised terms used in this DPA which are not defined above shall, unless stated otherwise, have the meaning given to them in the License Agreement.

## 2 General Provisions

2.1 You are the Controller (or Processor, as determined by Applicable Privacy Laws) of the Personal Data, and hereby authorise Supplier and its Affiliates to Process the Personal Data on Your behalf in connection with Supplier’s provision of the Services to Customer.

2.2 Each Party shall obtain and maintain all necessary permissions and/or consents that it requires under Applicable Privacy Laws to facilitate the lawful Processing

of the Personal Data and in accordance with the terms of this DPA and the License Agreement.

**2.3 CCPA Compliance.** If, and to only to the extent that, the CCPA applies, Supplier agrees that it shall (a) act solely as a “Service Provider” under the CCPA with respect to the Personal Data, and (b) not take any action that would result in the Supplier not acting as a Service Provider under the CCPA with respect to the Personal Data. Furthermore, Supplier shall not (i) sell the Personal Data, nor shall it (ii) retain, use, or disclose the Personal Data for any purpose other than for the specific purpose of providing the Services.

### **3 Supplier’s Obligations**

Supplier shall:

(a) only process the Personal Data on Your written instructions in accordance with Applicable Privacy Laws, this DPA and the License Agreement. Supplier is not responsible for determining if Your instructions are compliant with Applicable Privacy Laws. You hereby acknowledge that the Personal Data may be Processed on an automated basis in accordance with Your use of the Services, which Supplier does not monitor. Notwithstanding the aforesaid, if Supplier becomes aware that, in its reasonable opinion, Your instructions infringe Applicable Privacy Laws, we will notify You accordingly;

(b) keep the Personal Data confidential (in accordance with the confidentiality terms set out in the License Agreement), limit access to the Personal Data to authorized and properly trained personnel with a defined “need-to-know”, and ensure that persons authorised to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(c) taking into account the nature of the Processing, assist You by implementing and maintaining appropriate technical and organisational measures for the fulfilment of Your obligation to respond to requests for exercising the Data Subject's rights as stipulated in Applicable Privacy Laws;

(d) provide such assistance and information as may be reasonably requested to support Your compliance with its obligations pursuant to Applicable Privacy Laws and/or notices served by a Privacy Authority, including without limitation promptly assist You with responses to or providing information to Data Subjects and/or a Privacy Authority pertaining to the Processing of the Personal Data. If Supplier receives a notice from a Privacy Authority regarding any Personal Data Processed pursuant to this DPA, it shall, if permitted by applicable laws, (i) without delay notify You providing details of the Privacy Authority and the notice, and (ii) not respond to such

notice without Your prior approval of the proposed response;

(e) make available to You relevant information necessary to demonstrate compliance with the obligations laid down in this Section 3 and allow for, and contribute to, audits in accordance with Section 6.3 below (whether conducted by You (or Your appointed auditor) or a Privacy Authority;

(f) where technically possible (for some Services Processing is automated and Supplier may not store, retain or have ongoing access to the Personal Data once the Service has been provided): (i) promptly modify, correct, block, or delete Personal Data at Your request or as may be required by Applicable Privacy Laws; and at Your choice delete or return all the Personal Data to You after provision of the Services has ended, and delete existing copies, unless Applicable Privacy Laws require the retention or continued storage of the Personal Data by Supplier; and (ii) if requested, promptly provide You with a copy of an individual Data Subject’s Personal Data in intelligible form.

### **4 Your Obligations**

You shall:

(a) ensure that there is a lawful basis for Processing the Personal Data covered by this DPA, including that where consent is required from a Data Subject such consent is specific, informed and unequivocal;

(b) ensure that the Supplier does not receive or have access to Your data or confidential information other than the specific Personal Data to be Processed under this DPA (e.g. by You taking appropriate steps and implementing appropriate measures to safeguard files containing Your data and/or confidential information, such as segregating such files from systems connected to the Services, by making such files inaccessible through encryption, by anonymizing any data contained within them, etc.);

(c) promptly inform Supplier of any erroneous, rectified or updated Personal Data being processed by Supplier, as well as if any such data is to be deleted;

(d) in a timely manner, provide Supplier with lawful and documented instructions regarding Supplier's Processing of Personal Data;

(e) act as the Data Subject's sole point of contact.

### **5 Security of Processing**

**5.1** 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, both Parties shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

- (a) the pseudonymisation and encryption of Personal Data;
- (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and Services;
- (c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and
- (d) a process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

5.2 In assessing the appropriate level of security, account shall be taken of the risks that are presented by the Processing of the Personal Data, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise to be Processed by Supplier.

5.3 Supplier shall take steps to ensure that any natural person acting under the authority of Supplier who has access to the Personal Data does not Process such Personal Data otherwise than upon and in accordance with the instructions from Supplier unless he or she is required to do otherwise by Applicable Privacy Laws.

5.4 Supplier agrees to adhere to the technical and organisational measures referred to in Annex II of this DPA. If Supplier becomes aware of any non-conformity with such technical and organizational measures or of Applicable Privacy Laws, either within its own or a sub-processor's organization, it shall notify You without undue delay in writing of such non-conformity in accordance with the Personal Data Breach procedure set out in Section 9 below.

5.5 If any instructions, requests or other requirements issued by You pertaining to the Processing under this DPA require the Supplier to undertake extra activities and/or implement technical and organisational measures which, 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), exceed or are in addition to the reasonable activities and/or measures required to comply with Applicable Privacy Laws, and will cause an increase in operating costs for Supplier, Supplier shall be entitled to

claim compensation from You for that increased cost. The performance by the Supplier of such instructions, requests or requirements shall be subject to the Parties agreeing in writing on the reasonable and proper compensation due to Supplier for undertaking those extra activities and/or implementing those additional measures.

## 6 Sub-processors

6.1 You hereby give Supplier the general authority to sub-contract any Processing of Personal Data to a third party. Where Supplier engages a sub-contractor for the purpose of carrying out specific Processing activities on its behalf ("sub-processor"), Supplier undertakes to impose data protection obligations no less onerous than those set out in this DPA on that sub-processor in the form of a written agreement, which shall in particular provide sufficient guarantees that the sub-processor has implemented appropriate technical and organisational measures as required herein such that its Processing will meet the requirements of Applicable Privacy Laws. Supplier remains liable for its sub-processor's performance of its obligations and is responsible for any and all actions or omissions of such sub-processors.

6.2 A list of appointed sub-processors (as at the effective date of this DPA) is included in Annex III of this DPA.

6.3 Supplier shall notify You of any change to the list of sub-processors. You may (on reasonable data privacy related grounds) object to the use of a new sub-processor by giving written notice of such objection (including details of Your reasons) to Supplier within 14 calendar days of receiving notice of the appointment. Supplier will not transfer the Personal Data to a new sub-processor until the objection period has expired or if You have objected. To the extent a valid objection prevents or in any way hinders Supplier from providing any of the Services, the Parties shall discuss in good faith what alternative solutions (if any) are available to enable Supplier to continue providing affected Services.

## 7 Audit

Supplier shall, once per calendar year and upon request, make available to You such documented information as You may reasonably request demonstrating Supplier's compliance with the terms of this DPA and with Applicable Privacy Laws. If (and only to the extent that): (i) You cannot reasonably satisfy yourself of Supplier's compliance using the aforesaid information, or (ii) You have reasonable grounds for suspecting that there has been an unreported Personal Data Breach or that Supplier is in breach of the Processing provisions set out in this DPA, or (iii) where required by a relevant Privacy Authority or Applicable Privacy Laws, You may, upon giving Supplier prior written

notice, audit (or appoint a third party auditor to audit) at Your cost the technical and organizational security measures, systems, premises, access controls, etc. operated by Supplier that relate to the Personal Data being Processed by Supplier under this DPA, and which shall include where reasonable and appropriate, access to Supplier's Processing records and policies. You agree to give Supplier not less than 28 days' written notice of any information or audit request under this section (unless circumstances require that a shorter notice period be given, provided always that such notice period shall be reasonable). The Parties shall mutually agree on the details of the audit, including the reasonable start date, scope and duration of, and security and confidentiality controls applicable to, any such audit. The report generated from such an audit (and any information arising therefrom) shall be considered the Confidential Information of Supplier, and Customer may only share the same with a third party (including a third-party controller) with Supplier's prior written agreement.

## **8 International / Restricted Transfers**

**8.1 EU/EEA and Swiss Data Subjects.** Where the Processing of Personal Data relating to EU/EEA or Swiss Data Subjects does not take place (a) within the EU/EEA or Switzerland (as applicable) or (b) within a territory that has been designated by the European Commission or Switzerland (as applicable) as ensuring an adequate level of protection pursuant to the EU GDPR (or its successor) or the Swiss Data Protection Act (as applicable), such transfer and Processing of Personal Data shall be carried out in accordance with the then current SCCs, which shall be deemed incorporated into and form an integral part of this DPA in accordance with the Appendix hereto. An approved electronic execution or acceptance of this DPA shall be deemed as the "signature" of the Parties to the applicable SCCs. If any such transfer of Personal Data is to a sub-processor, Supplier shall procure that the terms of the applicable SCCs are imposed on such sub-processor before the transfer takes place. Information required by the SCCs is contained within the Appendix to this DPA.

**8.2 UK Data Subjects.** Where the Processing of Personal Data relating to UK Data Subjects does not take place (a) within the UK or (b) within a territory that has been designated by the UK as ensuring an adequate level of protection pursuant to the UK Data Protection Act (or its successor), such transfer and Processing of Personal Data shall be carried out in accordance with the then current SCCs together with a UK Addendum, which shall be deemed incorporated into and form an integral part of this DPA in accordance with the Appendix hereto. An approved electronic execution or acceptance of this DPA shall be deemed as the "signature" of the Parties to the

applicable SCCs and UK Addendum. If any such transfer of Personal Data is to a sub-processor, Supplier shall procure that the terms of the applicable SCCs and UK Addendum are imposed on such sub-processor before the transfer takes place. Information required by the SCCs and UK Addendum is contained within the Appendix to this DPA.

**8.3 All Other Data Subjects.** Cross-border transfers of Personal Data relating to Data Subjects from countries other than the EU/EEA, UK, or Switzerland and/or which originates from non-EU/EEA, non-UK, or non-Swiss jurisdictions (as applicable) shall be regulated by the Applicable Privacy Laws for the relevant jurisdiction(s) and shall be subject to the transfer mechanism(s) prescribed by those Applicable Privacy Laws. Notwithstanding the aforesaid, the Supplier's usual default transfer mechanism is the SCCs.

**8.4 Alternative Transfer Mechanisms.** If and to the extent that a court of competent jurisdiction or Privacy Authority (for whatever reason) determines that the measures described in this DPA cannot be relied on to lawfully transfer the Personal Data to Supplier, the Parties shall cooperate in good faith to agree and take any actions that may be reasonably required to implement any additional measures or alternative transfer mechanism to enable the lawful transfer of such Personal Data. In replacement or addition to the aforesaid, the Parties may agree to rely upon another approved transfer mechanism (e.g. approved binding corporate rules).

## **9 Personal Data Breaches**

**9.1** Supplier shall notify You without undue delay upon becoming aware of an actual or suspected Personal Data Breach. Such notice shall contain the following information (where known):

- (a) a description of the Personal Data Breach including a summary of the incident that caused the Personal Data Breach, the date and time of the relevant incident(s), the categories and number of Data Subjects concerned, the categories, nature, content, and number of data records concerned, and the physical location of the breach and the storage media involved;
- (b) a description of recommended measures to mitigate any adverse effects of the Personal Data Breach, and of the measures proposed or taken by Supplier (and sub-processor, as applicable) to address the Personal Data Breach;
- (c) a description of the likely consequences and potential risk that the Personal Data Breach may have towards the affected Data Subject(s);
- (d) any further information that may be relevant to the Personal Data Breach.

9.2 Depending on the nature of the Personal Data Breach, if You are obliged to make a report to a Privacy Authority in the country it resides, Supplier shall provide such further information as reasonably requested by You to support with the requests and/or enquiries from the Privacy Authority. Supplier shall not submit reports directly to any Privacy Authority unless this is expressly required by Applicable Privacy Laws or You have approved or instructed Supplier to submit its own report.

9.3 If You suspect a Personal Data Breach has occurred, You should contact Supplier without undue delay by sending an email to [security@mediakind.com](mailto:security@mediakind.com) with full details of the suspected breach.

## 10 Business contact details

Business contact details of each party and their respective staff, whether employees or contractors, whose information is provided to the other party in the course of performing its obligations under this DPA and/or the License Agreement shall only be Processed by the receiving party to the limited extent required to manage and administer the business relationship between the parties, in accordance with Applicable Privacy Laws.

## 11 Term and Termination

11.1 This DPA shall be effective from the date You first subscribe for the Services and shall remain in full force and effect for as long as Supplier Processes, or otherwise has access to, the Personal Data.

11.2 Either Party may terminate this DPA for cause if the other Party breaches any term of this DPA, provided always that (a) where such breach is capable of remedy, the breaching Party shall have thirty (30) days from receipt of written notice from the non-breaching Party to remedy such breach to the reasonable satisfaction of the non-breaching Party, and if not so remedied, or (b) if such breach is incapable of remedy, the non-breaching Party may immediately terminate this DPA upon written notice to the breaching Party.

11.3 Either Party may terminate this DPA immediately upon written notice if (a) a Party breaches the confidentiality provisions herein; or (b) a Party ceases its business, cannot pay its debts when due, or is subject to insolvency or bankruptcy proceedings; or (c) the License Agreement is terminated or expires.

## 12 Liability

12.1 Any limitations of liability set out in the License Agreement shall also apply to this DPA, save that nothing in this DPA or License Agreement shall (a) restrict a Party's rights under Applicable Privacy Laws to claim back

compensation paid to Data Subjects or (b) limit a Party's liability to the extent that such limitation violates any limits mandated by Applicable Privacy Laws.

12.2 Supplier shall have no liability in connection with, and hereby expressly disclaims all liability for, any claim, loss, damage, fine or penalty that arises in connection with this DPA, or related Processing activities, as a result (whether direct or indirect, or in part or whole) of any act, omission, instruction, or violation of this DPA, License Agreement or Applicable Privacy Laws by You.

## 13 Law and Jurisdiction

Save where the SCCs apply (in which event the law and jurisdiction stated therein shall apply), any dispute, controversy, proceedings or claim arising out of, or in connection with this DPA, shall be governed by the law, and exclusively resolved in the jurisdiction, stipulated in the License Agreement as applying to the Services for which the Personal Data is being Processed by Supplier.

## 14 Miscellaneous

14.1 Any provision of this DPA that expressly or by implication is intended to come into or continue in force on or after termination of this DPA shall remain in full force and effect, and in particular, the obligations set out in Sections 3(b) and 10 herein shall survive the expiry or termination of this DPA.

14.2 Notices pertaining to this DPA shall be served in accordance with the terms of the License Agreement, save that a copy of any such notices sent to the Supplier must also be sent by email to: [privacy@mediakind.com](mailto:privacy@mediakind.com).

14.3 No amendment of this DPA is effective unless it is in writing and signed by each Party.

14.4 In the event of a conflict between the terms of this DPA and the License Agreement, where this DPA stipulates that it prevails, or if the conflict relates to the subject matter of this DPA (being the Processing of the Personal Data by Supplier), the terms of this DPA shall prevail as to that conflict. In all other respects the terms of the License Agreement shall prevail.

14.5 Unless explicitly stated, the Parties intend that no person, other than the Parties, has any cause or right of action under this DPA.

14.6 If any provision of this DPA is held to be unenforceable: (a) that provision shall, where possible and permitted by law, be interpreted by modifying it to the minimum extent possible to make it, and (b) the remaining terms of this DPA shall remain in effect as written.

## APPENDIX EU STANDARD CONTRACTUAL CLAUSES & UK ADDENDUM

(Modules 2 and 3, as applicable)

Where Sections 8.1 and/or 8.2 of the DPA apply to a transfer of Personal Data to the Supplier, such transfer shall be governed by the SCCs, which shall be deemed incorporated into and form part of this DPA, as follows:

1. In relation to transfers of Personal Data protected by the EU GDPR, the SCCs shall apply as follows:
  - (a) where You are the Controller of the Personal Data, Module Two terms shall apply;
  - (b) where You are a Processor of the Personal Data, Module Three terms shall apply;
  - (c) in Clause 7, the optional docking clause shall apply and authorised Affiliates may accede the SCCs under the same terms and conditions as You, subject to mutual agreement of the parties;
  - (d) in Clause 9, "OPTION 2: GENERAL WRITTEN AUTHORISATION" is selected, and the process and time period for notice of sub-processor changes shall be as set out in Section 6.3 of this DPA;
  - (e) in Clause 11, the optional language shall not apply;
  - (f) in Clause 17, "OPTION 1" shall apply and the SCCs shall be governed by Irish law;
  - (g) in Clause 18(b), disputes shall be resolved before the courts of Ireland;
  - (h) Annex I shall be deemed completed with the information set out in Annex I of this DPA;
  - (i) Annex II shall be deemed completed with the information set out in Annex II of this DPA; and
  - (j) Annex III shall be deemed completed with the information set out in Annex III of this DPA.
2. In relation to transfers of Personal Data protected by the Swiss Data Protection Act, the SCCs as implemented under paragraph 1 above will apply with the following modifications:
  - (a) references to "Regulation (EU) 2016/679" and specific articles therein shall be interpreted as references to the Swiss Data Protection Act and the equivalent articles or sections therein;
  - (b) references to "EU", "Union", "Member State" and "Member State law" shall be replaced with references to "Switzerland" and/or "Swiss law" (as applicable);
  - (c) references to the "competent supervisory authority" and "competent courts" shall be replaced with references to the "Swiss Federal Data Protection Information Commissioner" and "applicable courts of Switzerland");
  - (d) the SCCs shall be governed by the laws of Switzerland; and
  - (e) disputes shall be resolved before the Swiss courts.
3. In relation to transfers of protected by the UK Data Protection Act, the SCCs as implemented under Section 1 above shall apply with the following modifications:
  - (a) the SCCs shall be modified and interpreted in accordance with the Mandatory Clauses set out in Part 2 of the UK Addendum, which shall be deemed incorporated into and form part of this DPA;
  - (b) Tables 1, 2 and 3 in Part 1 of the UK Addendum shall be deemed completed as required with the information set out in paragraph 1 above, and Annexes I, II and III of this DPA, as appropriate, and Table 4 in Part 1 of the UK Addendum shall be deemed completed by selecting "neither party"; and
  - (c) any conflict between the terms of the SCCs and the UK Addendum will be resolved in accordance with Sections 10 and 11 of the UK Addendum.

## **ANNEX I**

### **A. LIST OF PARTIES**

#### **Data exporter(s):**

Name:	<i>You (being the legal entity or person that subscribes to the Services in accordance with the License Agreement)</i>
Address:	<i>The address provided by You when setting up Your subscription account with Supplier</i>
Contact person:	<i>The name and contact details provided by You when setting up Your subscription account with Supplier</i>
Signature/Date:	<i>See section 11.1 of the DPA</i>
Role:	<i>Controller (where EU SCCs Module 2 applies) or Processor (where EU SCCs Module 3 applies)</i>

#### **Data importer(s):**

Name:	<i>The Supplier (being the MediaKind entity stated at the top of the DPA)</i>
Address:	<i>The Supplier's address stated at the top of the DPA</i>
Contact person:	<i>MediaKind DPO, <a href="mailto:privacy@mediakind.com">privacy@mediakind.com</a></i>
Signature/Date:	<i>See section 11.1 of the DPA</i>
Role:	<i>Processor (where EU SCCs Module 2 applies) or Subprocessor (where EU SCCs Module 3 applies)</i>

### **B. DESCRIPTION OF TRANSFER**

Categories of data subjects whose personal data is transferred / Categories of personal data transferred:

<b>Services</b>	<b>Categories of Data Subjects</b>	<b>Categories of Personal Data</b>
<i>MK.IO (account / configuration management)</i>	<i>Your personnel / Authorized Users (as defined in the License Agreement)</i>	<i>Account subscriber's name and email address; login credentials - userID, password (and possibly IP address and location) for account subscriber and allocated users</i>
<i>MK.IO (encoding / distribution)</i>	<i>As determined by You per Content file</i>	<i>Other Personal Data embedded in the Content as determined by You per Content file</i>
<i>MI.IO (support)</i>	<i>Your personnel</i>	<i>Support requestor's name and email address (and may include additional information such as job title, contact telephone number, work location, IP address)</i>

Special Categories of Personal Data may be Processed, as determined by You:

<b>Services</b>	<b>Categories of Data Subjects</b>	<b>Special Categories of Personal Data</b>
<i>MK.IO (encoding / distribution)</i>	<i>As determined by You per Content file</i>	<i>As determined by You per Content file</i>

Additional restrictions or safeguards applying to Special Category data, that takes into consideration the nature of the data and the risks involved:

*Encoding and distribution locations are chosen by You; all MK.IO encoding and distribution locations are on Microsoft Azure Cloud servers and as such any Personal Data stored on, accessed on or transiting through such servers are governed by Microsoft's privacy and security regime (including those additional restrictions and safeguards employed by Microsoft), the terms of which are viewable at this location: <https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA>*

Frequency of the transfer:

*Each Content file sent for encoding and distribution is a one-off transfer of the Personal Data embedded within that Content.*

Nature of the processing:

*Encoding / Distribution: Based on the configuration set by You, Supplier will retrieve Content files from Your chosen storage environment, move those files into a Supplier controlled environment, encode the file, and (at Your request) either return the file to Your chosen storage environment or distribute the file to Your end-users from a Supplier controlled server. You determine the location of the Supplier controlled environment and the manner of transfer (e.g. public or private network, Content protection utilised, etc.).*

*Support: Personal Data collected in connection with support requests / tickets raised by You are stored and analyzed by Supplier for the purpose of resolving the service incident to which the request / ticket relates.*

Purpose(s) of the data transfer and further processing:

*The encoding and distribution of Content files (as determined by You); together with the provision of support services, if requested.*

Period for which the personal data will be retained:

*Encoding / Distribution: The time required to encode and either return or distribute the Content (+ c.3-5 days with respect to Content for which a failed or error code is reported during encoding or distribution, for troubleshooting and/or support purposes).*

*Support: The period that Your subscription account is active plus up to 12 months thereafter.*

**Where the EU SCCs apply:**

## **C. COMPETENT SUPERVISORY AUTHORITY**

The competent supervisory authority in accordance with Clause 13 of the EU SCCs: *Ireland*

## **ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA**

The technical and organizational security measures that will apply to the Processing of the Personal Data under this DPA can be found [here](#).

## **ANNEX III – LIST OF SUB-PROCESSORS**

The controller has authorised the use of the following sub-processors:

<b>Full Name</b>	<b>Full Address</b>	<b>Contact Info</b>	<b>Services Provided</b>	<b>Scope of Processing</b>
Microsoft Corporation	One Microsoft Way, Redmond, Washington 98052, USA. Telephone: +1 (425) 882 8080	USA / ROW - Microsoft Enterprise Service Privacy, Microsoft Corporation (as left) Europe - Microsoft Ireland Operations, Ltd., Attn: Data Protection, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland	Cloud infrastructure (e.g. Azure Cloud); AI services (e.g. Azure AI Speech)	Storage, encoding infrastructure; AI services can include automated speech-to- text, speech translation, etc.
Zoho Corporation	4141 Hacienda Drive, Pleasanton, California 94588, USA	privacy@zohocorp.com	Support request/ticket logging (ZohoDesk)	Collection and storage of support request/ticket information