DATA PROCESSING AGREEMENT

MK.IO and MEDIAFIRST

This Data Processing Agreement ("DPA") is between the Supplier and Customer identified in an Order for MK.IO products and/or services and/or MediaFirst, in which case this DPA is deemed incorporated into and made a part of that Order. If any provisions of this DPA and the Order 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 Order remains unchanged and in full force and effect. Capitalised terms used in this DPA which are not defined herein shall, unless stated otherwise, have the meaning given to them in the Order.

BACKGROUND

(A) Customer will have access to MK.IO products and services and/or MediaFirst (defined collectively in the Order as "Products") that enable the reception, management and delivery of Content (including contribution, encoding, packaging, encryption, streaming, advertising services and storage), and in providing such Products to Customer it may be necessary for Supplier and/or its Affiliates to Process certain Personal Data on Customer's behalf.

(B) When setting up or configuring Products, Supplier will collect and Process limited Personal Data from Customer for the purpose of (i) facilitating the management and administration of Customer's account with Supplier, (ii) configuring the Products for use, and/or (iii) providing support services to Customer.

(C) If Customer is using Cloud Services, Supplier may Process Personal Data on Customer's behalf for various purposes as explained in this DPA, including Personal Data (i) relating to Customer's subscribers use of the Products, and (ii) embedded within Content that Customer chooses to encode in (and/or distribute from and/or store on, where applicable) Supplier's provided cloud environment. Customer determines what Personal Data is collected (or stored), 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 parameters related to Product use. 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 Customer.

(D) 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 its Authorized Users. Suppliers to the Supplier and its Affiliates are held to the same level of commitment when it comes to privacy.

(E) The terms and conditions specified herein shall apply if and when Supplier and/or its Affiliates Process Personal Data on Customer's behalf. Details of the Personal Data and proposed Processing activities are described in the Annexes to this DPA.

AGREED TERMS

1 Definitions

1.1 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:

Applicable Privacy Laws: 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);

Controller: the legal entity which, alone, on behalf of others, or jointly with others, determines the purposes and means of the Processing of Personal Data;

Data Subject: 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;

DPA: 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;

European Economic Area or EEA: 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);

Personal Data: any information relating to an identified or identifiable natural person (a "Data Subject") Processed under and in accordance with the terms of this DPA (as more particularly described in Annex I of this DPA);

Personal Data Breach: 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;

Privacy Authority: an independent regulatory or supervisory public authority with responsibility for privacy or data protection matters in a relevant jurisdiction;

Processing: 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);

Processor: the legal entity that Processes the Personal Data on behalf of the Controller;

SCCs or Standard Contractual Clauses: 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;

UK Addendum: 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.

2 General Provisions

2.1 Customer is 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 Customer's 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 Order.

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

(b) keep the Personal Data confidential (in accordance with the confidentiality terms set out in the Order), 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 Customer by implementing and maintaining appropriate technical and organisational measures to support Customer's obligation to respond to requests for exercising a Data Subject's rights as stipulated in Applicable Privacy Laws;

(d) provide such assistance and information as may be reasonably requested to support Customer's compliance with its obligations pursuant to Applicable Privacy Laws and/or notices served by a Privacy Authority, including without limitation promptly assist Customer 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 Customer providing details of the Privacy Authority and the notice, and (ii) not respond to such notice without Customer's prior approval of the proposed response;

(e) make available to Customer 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 7 below (whether conducted by Customer (or Customer's appointed auditor) or a Privacy Authority;

(f) where technically possible (for some Products 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 Customer's request or as may be required by Applicable Privacy Laws; and at Customer's choice delete or return all the Personal Data to Customer 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 Customer with a copy of an individual Data Subject's Personal Data in intelligible form.

4 Customer's Obligations

Customer 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 Customer's data or confidential information other than the specific Personal Data to be Processed under this DPA (e.g. by Customer taking appropriate steps and implementing appropriate measures to safeguard files containing Customer's 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 Customer 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 Customer 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 Customer 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 Customer 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 Customer of any change to the list of sub-processors. Customer 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 Customer's 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 Customer 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 Customer such documented information as Customer 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) Customer cannot reasonably satisfy itself of Supplier's compliance using the aforesaid information, or (ii) Customer 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, Customer may, upon giving Supplier prior written notice, audit (or appoint a third party auditor to audit) at Customer's 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. Customer 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, or which originates from, countries other than the EU/EEA, UK, or Switzerland 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 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 Customer 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 Customer 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 Customer 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 Customer have approved or instructed Supplier to submit its own report.

9.3 If Customer suspect a Personal Data Breach has occurred, Customer should contact Supplier without undue delay by sending an email to 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 Order 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 Customer places the Order with the Supplier 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 Order is terminated or expires.

12 Liability

12.1 The respective liability of the Parties under this DPA shall be subject to and form part of the limitations of liability set out in the Order, save that nothing in this DPA or Order 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, the Order or Applicable Privacy Laws by Customer.

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 Order 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 Order, save that a copy of any such notices sent to the Supplier must also be sent by email to: privacy@mediakind.com.

14.3 No amendment or variation 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 Order, 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 Order 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 Customer are the Controller of the Personal Data, Module Two terms shall apply;

(b) where Customer 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 Customer, 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:	*The Customer (as stated in the Order)*
Address:	*The address provided by the Customer in the Order*
Contact person:	*The name and contact details provided by Customer when setting up Customer's subscription account with Supplier*
Signature/Date:	*See section 11.1 of the DPA*
Role:	*Controller (where SCCs Module 2 applies) or Processor (where SCCs Module 3 applies)*

Data importer(s):

Name:	*The Supplier (as stated in the Order)*
Address:	*The address for the Supplier as stated in the Order*
Contact person:	*MediaKind DPO, privacy@mediakind.com*
Signature/Date:	*See section 11.1 of the DPA*
Role:	*Processor (where SCCs Module 2 applies) or Subprocessor (where SCCs Module 3 applies)*

B. DESCRIPTION OF TRANSFER

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

Services	***Categories of Data Subjects***	***Categories of Personal Data***
All MK.IO products and services (account / configuration management)	*Customer's personnel / administrative users*	*Authorized Users name and email address; login credentials (userID and password)*
If used: *MK.IO Beam (use);* *MediaFirst (on Customer infrastructure) (use)*	*As above*	*As above*
If used: *MK.IO Cloud Services (use, including encoding / distribution / storage)*	*As above*	*As above*
	Customer's subscribers and end-users	*Access logs containing user login credentials (for user traffic directed to MK.IO by Customer)*
	As determined by Customer and/or its subscribers and users per Content file	*Other Personal Data embedded in the Content as determined by Customer per Content file*
If used: *MK.IO Platform (use);* *MediaFirst (aaS) (use)* *(same as MK.IO Cloud Services, plus:)*	*Customer's subscribers and end-users*	*Subject to components used, and as determined by Customer, but may include:* *First and last name* *Email address* *Login credentials - User / Account ID and Password* *Physical Address* *IP Address* *Browser / Connection History*

Services	*Categories of Data Subjects*	*Categories of Personal Data*
		Subscriber Activity / History *Subscribed Services / Subscriptions* *GeoCodes / GeoLocation* *Purchase PIN* *Parental Control PIN* *Time Zone* *Devices* *TV / Channel Purchases / Rentals* *VOD / Live Activity* *Language* *Billing and Payment Information*
MK.IO support services	*Customer's personnel*	*Support requestor's name and email address (and may include additional information such as job title, contact telephone number, work location, IP address)*

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

Services	*Categories of Data Subjects*	*Special Categories of Personal Data*
If used: *MK.IO Cloud Services, Platform and/or MediaFirst (aaS) (use, including encoding / distribution / storage)*	*As determined by Customer and/or its subscribers and users per Content file*	*As determined by Customer per Content file*

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 (and if included, storage) server locations are chosen by Customer and will be dependant upon the cloud provider used (see Order, and Annex III below), and any Personal Data stored on, accessed on or transitting through such servers are subject to the additional restrictions and safeguards implemented by the cloud provider pursuant to their specific privacy and security regime(s).

Frequency of the transfer:

All MK.IO Products (incl. MK.IO Beam): Personal Data used for account management and product configuration will be collected as required.

MK.IO Cloud Services: For all cloud-based services, (i) Personal Data may be collected in connection with the Customer's (and its Authorized Users) use of cloud-based services, on a continuous basis, and (ii) for Content files encoded and/or distributed (and if storage is used, stored), is a one-off transfer of the Personal Data embedded within that Content.

If MK.IO Platform or MediaFirst (aaS) components are used, same as MK.IO Cloud Services above, and for subscriber/end-user data, as often as determined by Customer.

Nature of the processing:

All MK.IO Products (incl. MK.IO Beam): to set up or configure all MK.IO Products (including MK.IO Beam), Customer is required to create an online MK.IO account. Supplier will collect and Process limited Personal Data from Customer for the purpose of (i) facilitating the management and administration of Customer's account, (ii) configuring cloud-based services for use (e.g. including MK.IO Beam configuration and usage

management tools), and/or (iii) providing support services. Service administration is handled by the Customer and as such Customer personnel will have access to Supplier controlled service related tools that require login credentials (which may, if required from time to time, also include the administrators name, email address, and location information for security purposes).

MK.IO Cloud Services: per All MK.IO Products as above, plus - Customer chooses which MK.IO Cloud Services to use and when: encoding for live, event-based and/or video-on-demand streaming (including multiview composition), AI tools, advertising services, blackout controls, rights management, cloud storage and/or distribution/delivery services. Service administration and configuration is handled by the Customer. Based on the configuration(s) set by Customer, Supplier may retrieve Content files from Customer's chosen storage environment, move those files into a Supplier controlled environment (or if Supplier provides cloud storage for Content, Supplier will access those files from the Supplier controlled storage environment), encode the file, and (at Customer's request) either return the file to Customer's chosen storage environment or distribute the file to Customer's end-users from a Supplier controlled server and/or provide additional services (e.g. ad insertion, rights management, etc.) if requested by Customer. Customer determines the location of the Supplier controlled cloud environment (and if cloud storage is used, the storage location) and the manner of transfer (e.g. public or private network, Content protection utilised, etc.).

MK.IO Platform: per All MK.IO Products above, plus - MK.IO Platform is a cloud-native solution to ingest, encode, manage, distribute, and deliver Content (live/event-based, on-demand) using MK.IO Cloud Services, which, together with extra services such as cloud CDN, cloud subscriber account management, cloud billing/payment/user verification services, etc., can be tailored by the Customer to meet it's specific requirements. Service administration is handled by the Customer. The service collects, stores and processes end-user/subscriber information (as determined from time to time by Customer) to enable end-users/subscribers to access, browse and view Customer's Content, etc.

MediaFirst: per All MK.IO Products above, plus - as an end-to-end media platform (which can be cloud-based or on-premises, or a mix of both) MediaFirst is designed to enable customers to manage and deliver TV services to their consumers, which, together with optional add-ons such as a cloud CDN, cloud subscriber account management, and/or a cloud billing/payment service, can be tailored by the Customer to meet it's specific requirements. Service administration is handled by the Customer. The service collects, stores and processes end-user/subscriber information (as determined from time to time by Customer) to enable end-users/subscribers to access the Customer's TV service, browse and view Content, etc. Services and/or components thereof can be provided by Supplier as-a-service on a Supplier controlled public cloud environment (aka SaaS), or on a Customer controlled public cloud environment (aka MCA), or on non-cloud infrastructure at Customer premises, or on Customer provided cloud environments (private cloud).

MK.IO Cloud Servces, MK.IO Platform and MediaFirst (SaaS) include the ability to encode Content and such Content may contain embedded Personal Data, which Supplier may process during encoding (note for MediaFirst, Supplier does not process Content if encoding takes place on Customer's public cloud, private cloud or on-premises infrastructure). Customer chooses what Content to encode, and thus Customer determines what Personal Data it collects and hence what data elements are embedded within the Content. Supplier has no control over and has either no or limited visibility into the specific data elements of the Personal Data embedded within Content. Some of the optional components available may collect, store and process end-user/subscriber information (as determined from time to time by Customer), including (a) identity and access management ("user verification") for end-user login, authentication and authorization, (b) billing and payment, and (c) cloud-bsed CDN. For user verification, the service will only collect, store and process categories of Personal Data relevant to that purpose and to enable an end-user to self-manage its payment account; for billing and payment additional categories are required to enable record keeping and accurate billing (e.g. IP address, subscribed services / subscription history, purchases / rentals, payment history and information such as credit card or bank account details); and for cloud CDN, Content files will transit through and/or be cached on cloud-based CDN servers (user/subscriber IDs are anonymized on CDN servers).

MK.IO Support: Personal Data collected in connection with support requests / tickets raised by Customer 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:

Customer account management, service configuration; management, encoding and distribution of Content files, and/or if included, storage of Content on Customer's behalf (as determined by Customer); together with the provision of support services, if requested.

Period for which the personal data will be retained:

Personal Data collected for account management and configuration information will be retained for as long as Customer has active Orders, or the period that Customer's online account account is active, whichever is later; and in both cases, plus up to 12 months thereafter (to enable simple reactivation if required).

Personal data contained in subscriber/end-user access logs is retained for approximately 30 days (primarily for troubleshooting and/or support purposes).

If Supplier does not provide cloud storage, Content (and hence the Personal Data embedded therein) files encoded and/or distributed using cloud-based services will be retained for the time required to encode and either return or distribute the Content (plus c.3-5 days with respect to Content for which a failed or error code is reported during encoding or distribution, primarily for troubleshooting and/or support purposes).

If Supplier provides cloud storage, (i) Personal Data (excluding Personal Data embedded in Content) collected in connection with the Customer's (and its Authorized Users) use of cloud-based services will be stored for the period of the relevant Order, and (ii) for Content files, please refer to Supplier's resource documentation for each Product, which contains details of its default retention periods, and its archiving and retrieval policy, for Content files stored on a Supplier controlled cloud environment.

Personal Data collected in connection with support services will be retained for as long as Customer has active Orders, or the period that Customer's online account account is active, whichever is later; and in both cases, plus up to 12 months thereafter (to enable simple reactivation if required).

Where the SCCs apply:

C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority in accordance with Clause 13 of the 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:

Full Name	*Full Address*	*Contact Info*	*Services Provided*	*Scope of Processing*
If used: *Microsoft Corporation*	*One Microsoft Way, Redmond, Washington 98052, USA*	*USA / ROW - Microsoft Enterprise Service Privacy, Microsoft Corporation (address as left)* *EU - Microsoft Ireland Operations, Ltd., Attn Data Protection, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland* *Other contact details may apply by jurisdiction.* *Please go to: https://www.microsoft.com/privacy for more information*	*Cloud infrastructure; AI services*	*Storage, encoding infrastructure, AI services (can include automated speech-to-text, speech translation, etc.)*
If used: *Amazon Web Services, Inc.*	*410 Terry Avenue North, Seattle, WA 98109-5210, USA*	*USA / ROW - Amazon Web Services, Inc., (address as left), ATTN: AWS Legal* *EU – email: aws-EU-privacy@amazon.com / address: Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, L-1855, Luxembourg, ATTN: AWS Legal* *Other contact details may apply by jurisdiction.* *Please go to: https://aws.amazon.com/privacy/ for more information*	*Cloud infrastructure; AI services*	*Storage, encoding infrastructure, AI services (can include automated speech-to-text, speech translation, etc.)*
If used: *Google LLC*	*1600 Amphitheatre Parkway, Mountain View, California 94043 USA*	*Please go to: https://cloud.google.com/privacy for more information*	*Cloud infrastructure; AI services*	*Storage, encoding infrastructure, AI services (can include automated speech-to-text, speech translation, etc.)*
If used: *Zoho Corporation*	*4141 Hacienda Drive, Pleasanton, California 94588, USA*	*privacy@zohocorp.com* *Please go to:* *https://www.zoho.com/privacy.htm for more information I*	*Support request/ticket logging (ZohoDesk)*	*Collection and storage of support request/ticket information*
If used: *Slack Technologies, LLC*	*50 Fremont Street San Francisco, CA 94105, USA*	*privacy@slack.com* *USA / Canada - Slack Technologies, LLC (address as left)* *ROW - Slack Technologies Limited, Salesforce Tower 60 R801, North Dock, Dublin, Ireland* *Please go to:*	*Support requests handled via dedicated Slack channel*	*Collection and storage of support requests and channel discussions*

Full Name	Full Address	Contact Info	Services Provided	Scope of Processing
		https://slack.com/privacy for more information		
If used: *L&T Technology Services Limited*	*L&T Knowledge City, Special Economic Zone (IT/ITES), West Block – II, NH No. 8, Village Ankhol, Vadodara, Gujarat, 390019, India*	*dpo@ltts.com* *Please go to: https://www.ltts.com/data-privacy-policy for more information*	*Installation and deployment services; support services*	*Access to stored support requests; access to Customer's systems in connection with remote support activities*
For MK.IO Beam, if used: *Dell Technologies Inc. (and regional subsidiaries)*	*One Dell Way, Round Rock, Texas 78682, USA*	*privacy@dell.com* *Please go to: https:// https://www.dell.com and use the Privacy Statement link at the footer for country specific information*	*Support services*	*Access to stored support requests; access to Customer's systems in connection with remote or on-site support activities*
If MK.IO Multiview included: *See Order for details.*	*See Order for details.*	*See Order for details.*	*Compositing/dynamic layout services*	*Content encoding*
If Cloud CDN included: *See Order for details.*	*See Order for details.*	*See Order for details.*	*Cloud CDN services*	*Content in transit; cached Content*
If payment, billing and identity management services included: *See Order for details.*	*See Order for details.*	*See Order for details.*	*Payment, billing, and identity management services*	*Subscriber registration and verification; billing and payment collection*

See specific Orders to determine which products and/or services are included and/or in use, which specific sub-processors are being used, and which additional additional sub-processors are being used (if any).