DATA PROCESSING AGREEMENT

This Data Processing Agreement, including the annexes hereto, (the "**DPA**") is entered into between Kaltura, Inc., a Delaware corporation, having its principal place of business at 860 Broadway, 3rd Floor, New York, NY, 10003 USA ("**Kaltura**") on behalf of itself and the Kaltura Affiliates, and Customer on behalf of itself and its Affiliates. This DPA forms part of the Agreement (as defined below) between the parties and sets out the parties' agreement with respect to the Processing of Personal Data.

1. DEFINITIONS
   a. "**Affiliate**" means any entity controlling, under common control with, or controlled by either party, where "control" means ownership of more than 50% of the equity of such entity.
   b. "**Agreement**" shall mean, collectively, the Master License and Professional Services Agreement, the Kaltura Customer Agreement, or any other similarly titled services agreement and/or an executed Order Form and/or any other valid contract in force between Kaltura and Customer governing the Customer's use of the Services.
   c. "**Biometric Data**" shall mean Personal Data resulting from specific technical processing relating to the physical, physiological, or characteristics of a natural person, which allow or may allow confirmation of unique identification of that natural person, including but not limited to face data, facial geometry, and voice prints.
   d. "**Controller**" shall mean the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.
   e. "**Customer**" means the entity that enters into, or has entered into, the Agreement with Kaltura.
   f. "**Customer Admin**" means any of Customer's authorized staff, personnel, agents, employees, or Users who directly engage with Kaltura on behalf of Customer concerning their Kaltura account to use the Services.
   g. "**Customer Data**" shall mean Customer content, information, text, image, photos, as uploaded to the Kaltura platform, as well as any Input, Output (as defined below), including video, audio and images, that is Processed by Kaltura to the extent such content contains Personal Data, in the course of providing the Services, all as detailed in Annex 1 attached herein.
   h. "**Data Protection Regulations**" means all applicable and binding privacy and data protection laws and regulations, including Regulation (EU) 2016/679 of the European Parliament and of the Council (the "**GDPR**"), Regulation (EU) 2016/679 as it forms part of the law of the law of England and Wales, Scotland and Northern Ireland by virtue of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (SI 2019/419) (the "**UK GDPR**"), the Swiss Federal Act on Data Protection of 19 June 1992 and the Swiss Ordinance on the Federal Data Protection Act of 14 June 1993 (the "**FADP**"), the US Data Protection Laws (as defined below) and the Israeli Data Protection Laws (as defined below), known or reasonably expected by Kaltura to be applicable to the Processing of Personal Data hereunder and in effect at the time of Kaltura's performance hereunder.
   i. "**Data Subject**" shall mean an individual to whom the Personal Data relates.
   j. "**Deidentified Data**" shall mean information that cannot reasonably identify, relate to, describe, be capable of being associated with, be linked directly or indirectly with, or be reasonably be used to infer information about an identifiable natural person, all as defined under applicable US Data Protection Laws.
   k. "**Input(s)**" shall mean any data, content, text, audio, documentation, image, video, or information submitted, uploaded, or otherwise provided by or on behalf of Customer or Users to the Kaltura AI systems including, to the extent applicable, through integration with Customer's systems, or communications such as Chatbots, AI calls and conversations, etc.
   l. "**Instructions**" shall mean any reasonable, documented instructions given by Customer with respect to the lawful Processing of Personal Data. Instructions may include, without limitation, the correction, erasure and/or the blocking of Personal Data in the legal responsibility of the Controller. Customer may also give Instructions electronically by using the functionalities, settings, and preferences available within the Services.
   m. "**Israeli Data Protection Laws**" means, collectedly, the: (i) Israeli Protection of Privacy Law, 5741-1981 (as amended under Amendment 13); (ii) the regulations promulgated pursuant thereto, including the Israeli Protection of Privacy (Data Security) Regulations, 5777-2017 and the Israeli Protection of Privacy (Transfer of Data to Databases Abroad) Regulations, 5761-2001; (iii) any amendments or legislation replacing or updating any of the foregoing; and (iv) any judicial or administrative interpretation of any of the above, including any binding guidance, guidelines, codes of practice, approved codes of conduct or certification mechanisms approved by the Israeli Privacy Protection Authority.
   n. "**Output(s)**" means any data, content, or material generated by the Kaltura AI systems in response to Inputs submitted by Users, Customer Admin or otherwise individuals interacting with the Kaltura AI systems.
   o. "**Personal Data**" and/or "**Personal Information**" shall mean any information relating to an identified or identifiable natural person (a "**Data Subject**"), or Consumer (as defined in the CCPA, to the extent applicable) Processed by Kaltura solely on behalf of Customer in connection with the Services; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to the physical, physiological, mental, economic, cultural or social identity of that natural person.
   p. "**Processing**" and/or "**Process**" shall mean any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available,

alignment or combination, restriction, erasure or destruction.

q. "**Processor**" shall mean a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.

r. "**Sensitive Personal Data**" shall mean Personal Data that requires a higher level of protection under Data Protection Regulations, such as "special categories of personal data" under GDPR, "sensitive data" or other materially similar terms under applicable Data Protection Regulations.

s. "**Service(s)**" shall mean the Hosted Services, the Service Offerings, and/or any work, product, or service which Kaltura provides to Customer, Customer's Affiliates, and/or Users of any of the foregoing under the terms of the Agreement.

t. "**Sub-Processor**" shall mean (i) Kaltura, when Kaltura Processes Personal Data on behalf of Customer, and Customer itself is a Processor of such Personal Data, or (ii) Kaltura Affiliates and/or third-party processors engaged by Kaltura to Process the Personal Data, pursuant to Section 6 below.

u. "**SCCs**" refer to the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

v. "**US Data Protection Laws**" means any and all applicable federal and state privacy laws and regulations applicable to the Wonderful.ai Processing activities of Customer Data under this DPA, and any implementing regulations and amendment thereto, including without limitation the: (i) California Consumer Privacy Act (Cal. Civ. Code §§ 1798.100 - 1798.199) of 2018 including as modified by the California Privacy Rights Act as well as all regulations promulgated thereunder from time to time ('**CCPA**'); (ii) the Colorado Privacy Act C.R.S.A. § 6-1-1301 et seq. (SB 21-190) ('**CPA**'); (iii) the Connecticut Data Privacy Act, S.B. 6 (Connecticut 2022) ('**CTDPA**'); (iv) the Florida Digital Bill of Rights S.B 262 ('**FDBR**'); the Montana Consumer Data Privacy Act 68th Legislature 2023, S.B. 0384 ('**MTCDPA**'); the Oregon Consumer Data Privacy Act ORS 646A.570-646A.589 ('**OCDPA**'); (vii) the Texas Data Privacy and Security Act, Tex. Bus. & Com. Code Ann. § 541.001 et seq ('**TDPSA**'); (viii) the Utah Consumer Privacy Act, Utah Code Ann. § 13-61-101 et seq ('**UCPA**'); (ix) the Washington "My Health My Data" Act, Wash. Rev. Code § 19.373.005 et seq., and Nev. Rev. Stat. § 603A, as amended by Nevada S.B. 370 (together, the "**Washington and Nevada Consumer Health Data Laws**"); (x) the Virginia Consumer Data Protection Act, Va. Code Ann. § 59.1-575 et seq. (SB 1392) ("**VCDPA**"); (xi) the Delaware Personal Data Privacy Act ("**DPDPA**"), effective January 1, 2025; (xii) the Iowa Consumer Data Protection Act ("**ICDPA**"), effective January 1, 2025; (xiii) the Indiana Consumer Data Protection Act ("**INCDPA**"), effective January 1, 2026; (xiv) the Tennessee Information Protection Act ("**TIPA**"), effective July 1, 2025; (xv) the New Hampshire Data Privacy Act ("**NHDPA**"), effective January 1, 2025; (xvi) the Kentucky Consumer Data Protection Act ("**KCDPA**"), effective January 1, 2026; and (xvii) the Maryland Online Data Privacy Act ("**MODPA**"), effective October 1, 2025; and (xx) Oregon Consumer Data Privacy Act ("**OCPA**"). All as amended or superseded from time to time and including any implementing regulations and amendments thereto.

w. "**User**" means a natural person that uses the Services. Users can include employees, students or the audience of Customer, unless otherwise specified in an applicable Order Form.

x. The terms, "**Member State**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR. The terms "**Business**", "**Business Purpose**", "**Consumer**" and "**Service Provider**" shall have the same meaning as in the CCPA.
For the purpose of clarity, within this DPA "**Controller**" shall also mean "**Business**", and "**Processor**" shall also mean "**Service Provider**", to the extent that the CCPA applies. In the same manner, Processor's Sub-processors shall also refer to the concept of Service Provider.

Any capitalized terms used but not defined herein shall have the meanings ascribed to them in the Agreement.

2. DATA PROCESSING

a. **Roles of the parties.**

i. The parties acknowledge and agree that with respect to the Users' Personal Data, (1) Customer is the Controller and Kaltura is the Processor of Personal Data, or (2) Customer is the Processor and Kaltura is the Sub-Processor of Personal Data.

ii. For avoidance of doubt and without derogating from any other provisions in this Section 2, the parties acknowledge that with respect to Customer Admins' Personal Data, Kaltura acts as a separate independent Controller, and will process such Personal Data in accordance with Kaltura's Privacy Policy located at https://corp.kaltura.com/legal/privacy/privacy-policy/. Customer Admins' Personal Data may include the Customer Admins' name and Email address as detailed in the Privacy Policy.

b. **Kaltura's Processing of Personal Data.** Kaltura shall Process Personal Data under the Agreement only on behalf or under the instruction of Customer, and: (i) in accordance with the Agreement, this DPA, and Customer's reasonable Instructions, to the extent these Instructions are consistent with the terms of the Agreement in relation to the manner Processing shall be performed, (ii) as necessary to provide the Services, (iii) as required by laws applicable to Kaltura, and/or as required by a court of competent jurisdiction or other competent governmental or semi-governmental authority, provided that Kaltura shall inform Customer of the legal requirement before Processing, unless such law or order prohibit such information on important grounds of public interest, and (iv) in order to render Personal Data fully anonymous, non-identifiable and non-personal in accordance with applicable standards recognized by Data Protection Regulations and guidance issued thereunder.

c. **Instructions.** Kaltura shall inform Customer if, in Kaltura's opinion, a Customer's Instruction(s) for the Processing of Personal Data is unreasonable or contrary to applicable Data Protection Regulations, the Agreement, or this DPA. To the extent that Kaltura cannot, for any reason, comply

with an Instruction from Customer, (i) Kaltura shall inform Customer, providing relevant details of the issue, and (ii) Kaltura may, per its sole discretion, temporarily cease all Processing of the affected Personal Data (other than securely storing such Personal Data) and/or suspend Customer's access to the Services, without imposing any liability on Kaltura, (iii) the Parties will undertake prompt, good faith negotiations to resolve the issue(s) with the instructions, and (iv) if the Parties cannot agree on a good faith, reasonable resolution to the instruction issue in question and the costs thereof, Customer may, as its sole remedy, terminate the Agreement and this DPA with respect to the affected Processing, and Customer shall pay to Kaltura all the amounts owed to Kaltura. Customer will have no further claims against Kaltura (including, without limitation, requesting refunds for Services) pursuant to the termination of the Agreement and the DPA as described in this paragraph.

d. **Ownership of Personal Data.** As between Customer and Kaltura, all Personal Data Customer provides to Kaltura under the Agreement and this DPA, are the property of Customer.
e. **Deletion.** Upon termination of this DPA and the Agreement, the Personal Data shall be promptly destroyed or returned to Customer per its request. Where Customer has not expressed a request with respect to the return or deletion of Personal Data at the termination of this DPA, Kaltura shall destroy the Personal Data within a reasonable amount of time at its discretion, not to exceed 90 days from the termination of this DPA and/or the Agreement.
f. **Kaltura's Retention Policy.** Kaltura retains automatically archiving production and back-up logs in accordance with its internal policies and procedures for business operation and security purposes. Upon the expiry or termination of this DPA and the Agreement, to the extent that Kaltura's logs contain Personal Data, such Personal Data (i) shall not be further Processed by Kaltura, (ii) shall be protected by Kaltura in accordance with the terms of this DPA so long as Kaltura retains such Personal Data, and (iii) shall be destroyed in accordance with Kaltura's data retention policies.
g. **Details of the Processing.** The subject-matter of Processing of Personal Data by Kaltura is specified in Schedule 1 (Details of Processing) to this DPA.

3. DATA SECURITY
   a. **Security Measures.** Kaltura has implemented, and shall maintain, so long as Kaltura Processes Personal Data, technical and organizational measures set out in Annex 2, as may be amended from time to time, to protect the confidentiality, integrity, and accuracy of Personal Data.
   b. **Confidentiality.** Kaltura shall ensure that its personnel who have access to Personal Data are subject to a duty of confidentiality with respect to the Personal Data.
   c. **Security Incidents.**
      i. If Kaltura becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data (each a "**Security Incident**"), Kaltura shall, to the extent permitted by applicable law, notify Customer of such Security Incident without undue delay.
      ii. Kaltura shall take all steps it deems reasonable and necessary to remediate the cause of any Security Incident and mitigate its impact.
      iii. Kaltura shall provide any assistance reasonably required by Customer to comply with Customer's obligations under Data Protection Regulations to notify regulatory authorities and/or Data Subjects impacted by a Security Incident, to the extent the remediation and/or mitigation is within Kaltura's reasonable control. These obligations shall not apply to Security Incidents that are caused by Customer or anyone who uses the Services on Customer's behalf.
      iv. Customer will not make, disclose, release or publish any finding, admission of liability, communication, notice, press release or report concerning any Security Incident which directly or indirectly identifies Kaltura (including in any legal proceeding or in any notification to regulatory or supervisory authorities or affected individuals) without Kaltura's prior written approval, unless, and solely to the extent that, Customer is compelled to do so pursuant to applicable law. In the latter case, unless prohibited by such laws, Customer shall provide Kaltura with reasonable prior written notice to provide Kaltura with the opportunity to object to such disclosure and in any case, Customer will limit the disclosure to the minimum scope required.

4. CUSTOMER RESPONSIBILITIES
   a. Customer, in its use of the Services, and Customer's Instructions to Kaltura, shall comply with Data Protection Laws. Customer shall ensure that (i) it has established an appropriate legal basis to Process, and transfer Personal Data to Kaltura for Processing, in accordance with this DPA, the Agreement, and the Instructions, including obtaining express consent from the Data Subjects, to the extent required by Data Protection Regulations, (ii) all Data Subjects (including any Users) have been informed of the Processing and transfer to Kaltura of their Personal Data.
   b. Customer shall review the information Kaltura makes available regarding its data security, including the technical and organizational measures set out in Annex 2, and independently determine whether the Services are suitable for Customer's requirements.
   c. Kaltura makes available various security controls, features, and functionalities that Customer may choose to enable, as described in the Documentation. Customer is responsible for selecting and implementing the appropriate security measures for securing Personal Data.
   d. Customer shall not use the Services to Process any Sensitive Personal Data (excluding Biometric Data) where such Processing would impose on Kaltura any data security or data protection obligations that differ from or are in addition to those set out in the Agreement and this DPA.
   e. Customer shall use the Services in accordance to Kaltura's Acceptable Use Policy ("**AUP**"), available at https://corp.kaltura.com/legal/tos/acceptable-

use-policy/#, which is incorporated herein by reference. Customer agrees to comply, and to ensure that its Users comply, with the AUP at all times.

5. ASSISTANCE AND COOPERATION
   a. **Use of Services.** For the term of the Agreement and taking into account the nature of the Processing, Kaltura will provide Customer with the ability to correct, delete, or block Processing of Personal Data, or, upon Customer's Instructions, make such corrections, deletions, or blockages on Customer's behalf.
   b. **Data Subject Requests ,Privacy Impact Assessments and Prior Consultations**. Kaltura shall provide reasonable assistance to Customer with respect to (a) requests from Data Subjects exercising their rights to access, rectify, erase or object to processing of Personal Data pursuant to Data Protection Regulations; (b) privacy impact assessments carried out by Customer; and (c) Customer's prior consultations with Supervisory Authorities. Kaltura reserves the right to charge a fee for complying with a request for assistance requiring significant effort and/or resources.
   c. **Audits.**
      i. Kaltura will submit to an audit by an independent, reputable, third-party auditor ("Auditor") designated by Customer (provided that the Auditor is mutually agreed upon by the Parties and is not a competitor, or related to or controlled by a competitor, of Kaltura), to demonstrate Kaltura's compliance with this DPA, at Customer's sole expense, provided that Kaltura has been given reasonable prior notice, which shall not be less than twenty (20) business days. Customer shall require that the Auditor execute a standard confidentiality and nondisclosure agreement with Kaltura with respect to the confidential treatment and restricted use of information gathered in conducting the audit. If required by Data Protection Regulations, access to Kaltura's facilities by the Auditor shall be subject to Kaltura's reasonable access requirements and security policies.
      ii. Before conducting any audit, Kaltura shall make available all reasonable information necessary to demonstrate compliance with Customer's privacy, compliance, and information security obligations under this DPA. The Customer will take into consideration as proof of compliance with this DPA, relevant certifications (such as ISO or SOC), security questionnaires, or other relevant compliance reports held by, or produced for, Kaltura.
      iii. All audits, and any findings or reports resulting from any audit, shall remain subject to the confidentiality obligations set forth in the Agreement, shall only be used by Customer to assess compliance with this DPA, and shall not be used for any other purpose or disclosed to any third party without Kaltura's prior written approval.
      iv. Customer shall conduct no more than one such audit in any twelve-month period unless (1) otherwise required by Data Protection Regulations, or (2) due to a significant Security Incident. The Customer shall ensure that (x) any audit will not cause (or, if it cannot avoid, minimize) any damage, injury, or disruption to Kaltura's premises, equipment, personnel, and business/operations while conducting such audit or inspection, respecting a mutually agreed timeline, Kaltura's normal business hours, and scope, (y) maintain the Confidential Information of Kaltura's other customers, and (z) shall not compromise any of Kaltura's security policies.
      v. If the Customer is entitled, pursuant to any other contractual arrangement (e.g. the Agreement) to audit Kaltura's business for any other purpose, this clause shall not give rise to an additional audit by the Customer, but rather shall solely entitle the Customer to include the scope of this clause within the audit.

6. SUB-PROCESSORS
   a. **Appointment of Sub-Processors.** Customer acknowledges and agrees that: (a) Kaltura may engage Kaltura Affiliates as Sub-Processors, and (b) Kaltura and Kaltura Affiliates, on behalf of Kaltura, may each engage third parties as Sub-Processors to Process Personal Data on its behalf. Kaltura makes available to Customer the current list of applicable Sub-Processors used by Kaltura to Process Personal Data via https://corp.kaltura.com/legal/privacy/subprocessors-list. Such Sub-processor list includes the identities of those Sub-processors, the location of the Processing and the type of service rendered by each Sub-processor ("**Sub-Processor List**"). Additional optional Sub-Processors may be included in an Order Form approved by Customer. By entering into this DPA, the Sub-Processor List is hereby deemed authorized by Customer.
   b. **Purpose of Sub-Processing.** All Sub-Processors shall be permitted to Process Personal Data only as necessary to perform the services Kaltura has engaged them to provide and shall be prohibited from Processing Personal Data for any other purpose.
   c. **Agreements with Sub-Processors.** Kaltura or a Kaltura Affiliate has entered into a written agreement with each Sub-Processor containing data protection obligations no less protective of Personal Data than those in this DPA to the extent applicable to the nature of the services provided by such Sub-Processor.
   d. **Objection to new Sub-Processors.** Kaltura shall inform Customer of any intended addition or replacement of Sub-Processors prior to such addition or replacement. If Customer objects to such additional or replacement Sub-Processors for reasons relating to the protection of Personal Data to be Processed by the additional or replacement Sub-Processor, Customer must notify Kaltura in writing within 10 business days of Kaltura's such notice of replacement, and the parties shall negotiate in good faith to reach a mutually acceptable resolution. If the parties are unable to reach a mutually acceptable resolution, Customer's sole remedy shall be termination of the Agreement and this DPA with respect to the portion of the Services that cannot reasonably be provided by Kaltura without the use of the objected-to Sub-Processor. Failure to object to such new Sub-processor in writing within 10 business days following Kaltura's notice shall be deemed acceptance of the new Sub-Processor.
   e. **Kaltura's responsibilities for Sub-Processors.** Kaltura shall remain at all times responsible to

Customer for the Sub-Processors' compliance with this DPA.

7. CROSS-BORDER DATA TRANSFERS
   a. Customer acknowledges and agrees that Kaltura may Process Personal Data globally to the extent necessary to provide the Services and to fulfil Kaltura's other obligations under the Agreement. To the extent any Personal Data subject to the GDPR, the UK GDPR, or the FADP is Processed by Kaltura outside the European Economic Area, the United Kingdom, or Switzerland, respectively ,or any country deemed to offer an adequate level of data protection under or pursuant to the adequacy decisions published by the European Commission, the UK Secretary of State or the applicable Swiss authority, as applicable ("**Adequacy Decision**"), such Personal Data shall be transferred on the basis of such Adequacy Decision without any further safeguards being necessary. If the Processing of Personal Data by Kaltura includes a transfer (either directly or via onward transfer) from the EEA, the UK, or Switzerland to other countries which have not been subject to a relevant Adequacy Decision, and such transfers are not performed through an alternative recognized compliance mechanism as may be adopted by Kaltura for the lawful transfer of personal data (as defined in the GDPR, the UK GDPR or the FADP, as relevant) outside the EEA, the UK or Switzerland, as applicable, then such transfers shall be made in accordance with Sections 7.b – 7.d below.
   b. Where a transfer of Personal Data is subject to the GDPR or the FADP, the SCCs shall apply. The SCCs shall be incorporated by reference into this DPA and completed as follows:
      i. The text of module 2 (Controller to Processor) shall apply where Customer is the Controller, and Kaltura is the Processor. The text of module 3 (Processor to Processor) shall apply where Customer is the Processor, and Kaltura is the Sub-Processor;
      ii. The optional docking clause of clause 7 shall apply;
      iii. In clause 9(a), option 2 shall apply. The time period for providing advance notice of any intended changes to the list of Sub-Processors shall be as set forth in section 6(d) to this DPA;
      iv. In clause 11(a), the optional language shall not apply;
      v. In clause 17, option 1 shall apply, and the SCCs shall be governed by the laws of the Republic of Ireland;
      vi. In clause 18(b), any dispute arising from the SCCs shall be resolved by the courts of the Republic of Ireland; and
      vii. The information required by Annex I and Annex II of the SCCs shall be as set out in Annex 1 and Annex 2 of this DPA, respectively.
   c. Where a transfer of Personal Data is subject to the FADP, in addition to the provisions of Section 7.b above, the following terms shall apply:
      i. The terms "General Data Protection Regulation" or "Regulation (EU) 2016/679" as utilized in the EU SCCs shall be interpreted to include the FADP with respect to Swiss Transfers;
      ii. The term "Union", "EU" and "EU Member State" in the SCCs shall not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the SCCs; and
      iii. The Swiss Federal Data Protection and Information Commissioner shall act as the "competent supervisory authority" insofar as the relevant data transfer is governed by the FADP, and the SCCs shall be governed by Swiss law and subject to the jurisdiction of the courts of Switzerland.
      iv. Where Swiss Transfers are exclusively subject to the FADP, all references to the GDPR in the EU SCCs are to be understood to be references to the FADP;
      v. Where Swiss Transfers are subject to both the FADP and the GDPR, all references to the GDPR in the EU SCCs are to be understood to be references to the FADP insofar as the Swiss Transfer is subject to the FADP.
   d. Where a transfer of Personal Data is subject to the UK GDPR, the SCCs shall apply, as amended by the UK Addendum to the SCCs issued by the Information Commissioner's Office under s.119A(1) of the UK Data Protection Act 2018 and attached hereto as Annex 3.
   e. To the extent any provision of this DPA contradicts or is inconsistent with the terms of the SCCs with respect to the transferred Personal Data, the terms of the SCCs shall prevail, and the inconsistent provision of this DPA shall be deemed amended accordingly.
   f. If, at any time:
      i. the laws or regulatory procedures of any jurisdiction require any further steps to be taken in order to permit the transfer of Personal Data as contemplated under this DPA (including, without limitation, executing or re-executing the SCCs as a separate document setting out the proposed transfers of Personal Data, and entering into additional cross-border transfer clauses); and/or
      ii. the transfer mechanisms in this Section 7 are (i) amended, replaced or repealed under Data Protection Regulations, (ii) declared invalid by a court of competent jurisdiction, or (iii) otherwise terminated, annulled, replaced or repealed under Data Protection Regulations;

      then the parties shall work together to take all steps reasonably required and negotiate in good faith any other solution to enable a transfer in compliance with Data Protection Regulations.

8. CALIFORNIA CONSUMER PRIVACY ACT.
   Kaltura acknowledges and confirms that it does not receive or process any Personal Information as consideration for any services or other items that Kaltura provides to Customer under the Agreement. As may be applicable to the Services provided under the Agreement, Kaltura certifies that it understands the rules, requirements and definitions of the CCPA and agrees to refrain from selling or sharing (as such terms are defined in the CCPA) any Personal Information Processed hereunder, without Customer's prior written consent or instruction, nor take any action that would cause any transfer of Personal Information to or from Kaltura under the Agreement or this DPA to qualify as "selling" and/or "sharing" such Personal Information under the CCPA. Kaltura acknowledges that Customer discloses Personal Information to Kaltura only for limited and

specified business purposes (as such term is defined in the CCPA) set out in this DPA and the Agreement. Kaltura shall process all Personal Information only (i) for such limited and specific business purpose(s), and (ii) in compliance with applicable sections of the CCPA, in a manner that provides the same or materially similar level of privacy protection as required of Customer considering the Personal Information processed and industry standards.
Kaltura shall not (i) retain, use, or disclose Personal Information outside the direct business relationship of the parties, as described in the Agreement, or for any business or commercial purpose other than for the specific business purpose of performing the Services or as otherwise permitted by the Agreement and/or this DPA, nor (ii) combine Personal Information with personal information Kaltura processes on behalf of other parties unless expressly permitted under the CCPA and the Agreement between the parties.
As applicable to the Services provided, Kaltura shall implement reasonable security measures, as described in Section 3 of this DPA, as appropriate under the CCPA, and reasonably assist Customer or otherwise enable Customer to comply with its obligations relating to any request received from an individual under the CCPA, as described in Section 5 of this DPA. Customer shall inform Kaltura of any request received from an individual under the CCPA which requires Kaltura's assistance in order to be fulfilled by Customer, and shall provide Kaltura all information necessary for it to assist with the request.
Subject to the audit provisions in the Agreement and this DPA, Kaltura acknowledges that Customer has the right to take reasonable and appropriate steps to ensure that Kaltura uses Personal Information in a manner consistent with Customer's obligations under the CCPA.
Kaltura further acknowledges that Customer has the right, upon notice, to take reasonable and appropriate steps to stop and remediate any unauthorized use of Personal Information by Kaltura, subject to the conditions agreed upon in this DPA, including audit provisions. Kaltura shall notify Customer if Kaltura makes a determination that it can no longer meet its obligations under the CCPA.
.

9. THIRD PARTY REQUESTS FOR ACCESS
Unless prohibited by applicable law, Kaltura shall promptly inform Customer of any request, correspondence, inquiry, or complaint received by Kaltura from a Data Subject, Supervisory Authority, or other third party in connection with Kaltura's Processing of Personal Data. Kaltura shall not respond to such requests without Customer's prior consent, except where legally required or to confirm its receipt.

10. LIMITATION OF LIABILITY
The liability of each party and its respective Affiliates arising out of or related to this DPA and the Agreement shall not, when taken together in the aggregate, exceed the limitation of liability set forth in the Agreement.

11. MISCELLANEOUS
a. If any provision in this DPA is found to be ineffective or void, this shall not affect the remaining provisions. The parties shall replace the ineffective or void provision with a lawful provision that reflects the business purpose of the ineffective or void provision. The parties shall similarly add necessary and appropriate provisions where such provisions are missing.
b. The governing law of this DPA will be the same as the governing law identified in the Agreement.
c. This DPA prevails over any additional, conflicting, or inconsistent terms and conditions appearing in the Agreement and/or any document submitted by either party regarding the Processing of Personal Data.
d. This DPA and its annexes set out the entire agreement and understanding between the Parties and supersede all previous proposals, agreements, and other communications between the parties (whether written, oral or otherwise) in relation to the subject matter of this DPA or regarding the Processing of Personal Data. This DPA may be modified, supplemented, or amended only by a written agreement signed by both parties thereto.
e. By using the Services, Customer accepts this DPA and the undersigned represents and warrants that it has full authority to bind the Customer to this DPA. If the undersigned cannot, or does not agree to, comply with and be bound by this DPA, or does not have authority to bind the Customer or any other entity, please do not use the Services.
f. This DPA shall become effective upon its execution (the "**DPA Effective Date**") and shall automatically terminate upon the termination or expiration or the Agreement in accordance with the terms therein.

Both parties accept the terms of this DPA by signing below.

Each party has read, understands, and agrees to the terms of this DPA. The parties agree that this DPA may be electronically signed, and that any electronic signatures appearing on this DPA are the same as handwritten signatures for the purposes of validity, enforceability, and admissibility. This DPA may be executed in counterparts, each of which shall be an original and all of which, when taken together, shall constitute one and the same instrument.

AGREED TO AND ACCEPTED BY:

Kaltura, Inc.	**Customer:**
Signature:	Signature:
Name:	Name:
Position:	Position:
Date:	Date:

ANNEX 1

Details of the Processing

A. LIST OF PARTIES

Data exporter:

- Name: Customer's entity name as identified in the Agreement
- Address: Customer's address as specified in the Agreement
- Contact person's name, position and contact details: Customer's contact details as specified in the Agreement
- Activities relevant to the data transferred under these Clauses: Receipt of the Services
- Signature and date: These Clauses shall be deemed executed and entered into by Customer as of the DPA Effective Date.
- Role: The data exporter's role shall be Controller or Processor specified in Section 2.a of the DPA.

Data importer:

- Name: Kaltura, Inc.
- Address: 860 Broadway, 3rd Floor, New York, NY 10003 USA
- Contact person's name, position and contact details: Kaltura Data Protection Officer, DPO@kaltura.com
- Activities relevant to the data transferred under these Clauses: Provision of the Services
- Signature and date: These Clauses shall be deemed executed and entered into by Kaltura as of the DPA Effective Date.
- Role: The data importer's role shall be Processor.

B. DESCRIPTION OF TRANSFER

Categories of Data Subjects
The categories of Data Subjects include the Customer and the Users who use the Services, as well as any individual whose Personal Data is uploaded by the Customer or its Users as part of the Input while using the Services.

Categories of Personal Data Processed

1. Any content, information, text, audio, photo, images, videos or other materials submitted through the Services (including the within the Input), which may contain Personal Data submitted by the Customer. The extent of such Personal Data is determined and controlled solely by the Customer. Categories of Personal Data processed may include: Technical identifiers, including user IDs, user agents, and IP addresses;
2. The names and email addresses of Users in cases where Customer's User authentication configuration requires this information;
3. Where Services include virtual event registration, any Personal Data contained in event registration forms;
4. Account activity (including media files uploaded, recorded live sessions, viewing history, likes and comments, chat history in live meeting solutions, account analytics, and any quizzes taken);
5. Recording data (including video, audio, and screen recordings), face data, audio data, and other biometric data (including potentially Biometric Data), to the extent captured, processed, or stored by the Services as enabled by Customer or the Users; and Any Personal Data contained in media content and metadata uploaded to, or transmitted via, the Services by Customer or its Users.

Special Categories of Data
The Services are not intended for Processing of Sensitive Personal Data, and the Customer agrees that such Sensitive Personal Data is not included in the scope of the Processing or Services being provided to the Customer. However, to the extent Kaltura AI systems are used, through certain features Kaltura may process on Customer's behalf Biometric Data, which could be defined in certain jurisdictions as Sensitive Data.

Duration and Frequency of the Processing
Processing shall take place on a continuous basis so long as Kaltura continues to provide the Services to Customer in accordance with the Agreement.

Nature and Purpose of the Processing
Personal Data is Processed for the purpose of providing the Services as set out in the Agreement. Processing activities may include:

1. Where Customer selects Kaltura's standard SaaS offering, hosting of Customer's media content, metadata, and User data on secure data centers located in the United States; where Customer selects one of Kaltura's regional SaaS offerings, hosting of Customer's media content, metadata, and User data on secure data centers located in Ireland, Canada, Singapore, or Australia, as applicable. Customer's media content and metadata may contain Personal Data.
2. Processing and transcoding of media content and metadata, and transmission of data over the internet and/or private networks to Users via the Services. Processing network traffic and activity on the Services may involve Personal Data of individuals interacting with the Services. Processing activities may be performed through Sub-Processors. Processing may take place in any jurisdiction where Users interact with the Services.
3. Performing maintenance and support services on systems which may contain Personal Data or in connection with the Services.
4. Managing Customer's account with Kaltura.

Personal Data Retention Period
Personal Data shall be retained by Kaltura for the duration of the Agreement, or as long as it is necessary in order to provide the Services.

Sub-Processors
With respect to Sub-Processors engaged by Kaltura:

1. The nature and purpose of the Processing is to enable provision of the services that Kaltura has engaged the Sub-Processors to provide. Each Sub-Processor Processes Personal Data solely to the extent necessary to provide the contracted services.
2. The subject matter of the Processing may include providing (i) cloud computing infrastructure, (ii) logs analysis, (iii) content delivery network (CDN) services, (iv) content transcription, translation, and captioning services, (v) customer service and support, (vi) virtual or hybrid event management services, and (vii) other optional functions that Customer chooses to enable and/or use via the Services.
3. The duration of the processing shall be for the duration of the Agreement.

To obtain the current list of Sub-Processors applicable to the Services provided to Customer, please visit https://corp.kaltura.com/legal/privacy/subprocessors-list/.

C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority shall be as determined by the GDPR except insofar as the Processing is subject to the FADP, in which case the competent supervisory authority shall be the Federal Data Protection and Information Commissioner of Switzerland, or the UK GDPR, in which case the competent supervisory authority shall be the UK's Information Commissioner's Office.

Annex 2

Technical and Organizational Security Measures

Technical Measures

a. **Information Security Program and Certifications**: Kaltura maintains documented security policies and procedures which are reviewed and updated on a regular basis. The Kaltura platform is certified compliant with the ISO27001 and ISO27799 information security management standards. The scope of the certification encompasses Kaltura's production environments, corporate environments, and operations. Kaltura's platform is hosted on public cloud infrastructure operated by leading cloud providers that are SOC-1 (formerly SSAE 16) and SOC-2 Type II certified.

b. **Encryption**: Customer data is encrypted at-rest and in while transit over public or wireless networks using industry standard encryption protocols.

Organizational Measures

a. **Policies and Procedures for Government Access**: Kaltura has implemented policies and procedures to manage and respond to requests from government agencies for access to customer data. These policies and procedures include determining whether each request is valid, legally binding and lawful, and notifying the affected customer unless prohibited by applicable laws.

b. **Data Minimization**: Kaltura collects and processes personal data only to the extent necessary to provide Kaltura products and services to customers.

c. **Sub-Processors**: Prior to engaging a sub-processor, Kaltura reviews the sub-processor's business and operations, including the sub-processor's security, privacy, and compliance practices. With respect to each sub-processor that has access to customer data, Kaltura remains accountable to the customer for the sub-processor's acts and omissions.

Customer may request Kaltura's latest security policies for review by contacting DPO@kaltura.com.

Annex 3

UK International Data Transfer Addendum to the EU SCCs

Part 1: Tables

Table 1: Parties

Start date	DPA Effective Date	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Customer	Kaltura
Key Contact	Please see Annex 1 of this DPA	Please see Annex 1 of this DPA
Signature (if required for the purposes of Section 2)	Customer's signature to this DPA shall be deemed its signature of this UK Addendum.	Kaltura's signature to this DPA shall be deemed its signature of this UK Addendum.

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	The version of the Approved EU SCCs to which this Addendum is appended is as described in Section 7.b of this DPA.

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this UK Addendum is set out in Annexes 1 and 2 of this DPA.

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: Importer and Exporter

Part 2: Mandatory Clauses

Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 28 January 2022, as it is revised under Section 18 of those Mandatory Clauses.