DATA PROCESSING AGREEMENT

Last Updated: April 15, 2026

This Data Processing Agreement (this "**DPA**") is entered into by and between Customer and the Panopto entity(ies) specified in Section 1.7 below and establishes the parties' respective responsibilities under Data Protection Laws (as defined below) with respect to Personal Data to be processed by Panopto pursuant to the Technology Services Agreement or other written agreement entered into by the parties with respect to Panopto's provision of, and Customer's use of, the Services (the "**Agreement**"). By executing the Agreement referencing this DPA, Customer acknowledges that this DPA is an addendum to, and forms a vital part of, the Agreement.

1. **Definitions**. Capitalized terms used but not defined in this DPA will have the meanings ascribed to them in the Agreement. In this DPA, the following initially capitalized terms will have the meanings set out below.

   1.1. "**Customer**" means the party that purchases or uses the Services pursuant to the Agreement.

   1.2. "**Data Protection Laws**" means any data protection laws or regulations applicable to Panopto's processing of the Personal Data under this DPA, including, but not limited to: (a) EU Area Law; (b) the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Acts of 2020 ("**CCPA**"); (c) any laws or regulations ratifying, implementing, adopting, supplementing or replacing the foregoing; and (d) any guidance or codes of practice issued by a governmental or regulatory body or authority in relation to compliance with the foregoing; in each case, to the extent in force, and as such are updated, amended or replaced from time to time.

   1.3. "**Data Subject Request**" means a request from a Data Subject to exercise their data subject rights under Data Protection Laws, including, but not limited to, those data subject rights under Chapter 3 of the GDPR.

   1.4. "**DPA Effective Date**" means the date of the Agreement is effective.

   1.5. "**EU Area**" means the European Union, the European Economic Area, United Kingdom ("**UK**"), and Switzerland.

   1.6. "**EU Area Law**" means (a) the Regulation (EU) 2016/679 ("**GDPR**"); (b) the GDPR as amended and incorporated into UK law under the UK European Union (Withdrawal) Act 2018 and as amended by Schedule 1 to the Data Protection, Privacy and Electronic Communication (Amendments etc.) (EU Exit) Regulations 2019 (SI 2019/419) (the "**UK GDPR**"); (c) the Revised Swiss Federal Act on Data Protection of 25 September 2020 ("**FADP**"); (d) any successor or amendments thereto (including, without limitation, implementation of GDPR by Member States into their national law); or (d) any other law relating to the data protection, security, or privacy of individuals that applies in the EU Area.

   1.7. "**Panopto**" means, if Customer purchases Panopto Services, the Panopto entity identified as follows based on Customer's account region: (a) if Customer is located in the Americas, Panopto, Inc.; (b) if Customer is located in Europe, the Middle East, or Africa, Panopto EMEA Limited; (c) if Customer is located in Australia or New Zealand, Panopto ANZ Pty Ltd; (d) if Customer is located in Hong Kong, Panopto Asia Pacific Limited; or (e) if Customer is located in Asia-Pacific (excluding Australia, New Zealand, and Hong Kong), Panopto Asia Pte Ltd. "Panopto" means, if Customer purchases Elai Services, and regardless of Customer's location, Elai Inc.

   1.8. "**Personal Data**" means any data which (a) qualifies as "Personal Data", "Personal Information", "Personally Identifiable Information" or any substantially similar term under applicable Data Protection Laws and (b) is processed by Panopto on behalf of Customer in connection with the Agreement.

   1.9. "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

   1.10. "**Personnel**" means any personnel of Panopto who are authorized to process Personal Data under the authority of Panopto.

   1.11. "**Services**" means the services provided by Panopto to Customer pursuant to the Agreement.

   1.12. "**Standard Contractual Clauses**" or "**SCCs**" means, as applicable, (a) the standard contractual clauses for the transfer of European Area Personal Data to Third Countries annexed to the European Commission's Decision (EU) 2021/914 of 4 June 2021 currently found at https://eur-lex.europa.eu/eli/dec_impl/2021/914, as modified by Section 7.2.3 and as may be amended, superseded, or replaced, and/or (b) the International Data Transfer Addendum to the EU

Commission standard contractual clauses issued by the UK Information Commissioner under section 119A(1) of the UK Data Protection Act 2018 currently found at https://ico.org.uk/media2/migrated/4019539/international-data-transfer-addendum.pdf ("**UK Addendum**"), as modified by Section 7.2.3 and as may be amended, superseded, or replaced.

1.13. "**Sub-Processor**" means any third party appointed by or on behalf of Panopto in connection with the processing of Personal Data in connection with the Agreement.

1.14. "**Third Country**" means (a) a country or territory that has not received an adequacy decision relating to data transfers from the European Commission as further set forth in the GDPR, and/or (b) a country or territory that does not have "essentially equivalent" privacy laws as further set forth in the UK GDPR.

1.15. In this DPA, the following terms (and any substantially similar terms as defined under Data Protection Laws) shall have the meanings and otherwise be interpreted in accordance with Data Protection Laws: **Business**, **Controller**, **Data Controller**, **Data Processor**, **Data Subject**, **Processor**, **Sell**, **Service Provider**, **Sub-Processor**, **process(ing)** and **transfer**.

2. **Scope of DPA**.

2.1. Scope. This DPA applies where and solely to the extent that Panopto processes Personal Data in accordance with the Agreement (the "**Business Purpose**"). The subject matter and duration of the processing, nature and purpose of the processing, type of Personal Data and categories of Data Subjects are set out in Exhibit A attached hereto, which is hereby incorporated by reference. The Parties acknowledge that the requirements set forth in this DPA apply only to Personal Data in identifiable form, and that such requirements do not apply to information which does not relate to an identified or identifiable natural person or to Personal Data rendered anonymous in such a manner that the Data Subject is no longer identifiable.

2.2. Role of the Parties. As between Customer and Panopto, Customer is the Controller or Processor, as the case may be, of the Personal Data, and Panopto is the Processor or Sub-Processor, as the case may be, of the Personal Data processed in connection with Customer's access to and use of the Services.

2.3. Compliance with Data Protection Laws. Customer and Panopto will each comply with its respective obligations under Data Protection Laws in connection with the processing of Personal Data. In connection with its access to and use of the Services, Customer shall process Personal Data within the Services and provide Panopto with instructions in accordance with Data Protection Laws.

3. **Customer's Obligations**.

3.1. General. Customer represents and warrants to Panopto that (a) Customer will remain duly and effectively authorized to give the Instructions (defined below) set out in the Agreement, this DPA, or as Customer otherwise provides; and (b) Customer retains responsibility for responding, and Customer will promptly respond, to any inquiries regarding the Personal Data, including without limitation any and all Data Subject Requests.

3.2. Data Quality and Integrity. Customer is solely responsible for the accuracy, quality, and legality of (a) the Personal Data provided to Panopto by or on behalf of Customer, the nature, scope, or origin of, or the means by which, Customer acquired such Personal Data, or (c) the Instructions (as defined below) it provides to Panopto regarding the processing of such Personal Data. Customer shall not provide or make available to Panopto any Personal Data in violation of the Agreement or Data Protection Laws or otherwise inappropriate for the nature of the Services.

3.3. Notice and Choice. Customer is solely responsible for providing its end users with appropriate notice regarding its processing activities. Customer retains sole responsibility for the collection and maintenance of all necessary consents and rights for, the necessary or appropriate pseudonymization or deidentification of, and the lawful and appropriate use of any Personal Data and Sensitive Personal Data included in, or referenced by, Customer Content, comments on or references to that Customer Content, and configuration of the Services to restrict viewing access to the Customer Content, where applicable, including without limitation all necessary consents, licenses, or approvals for the processing of, or otherwise having a valid legal basis under Data Protection Laws for the processing of, any Personal Data provided by Customer or its end users to Panopto in connection with the Services. Customer also retains responsibility for the creation, maintenance, and testing of any backups for Customer Content.

4. **Panopto's Obligations**.

4.1. Instructions. Customer instructs Panopto (and authorizes Panopto to instruct its Personnel and Sub-Processors) to process the Personal Data, including with regard to transfers of Personal Data to a Third Country or an international organization, for the Business Purpose and in a manner consistent with the Agreement, this DPA, and Data Protection Laws (collectively, the "**Instructions**"). Panopto shall not Sell Personal Data or retain, use or disclose the Personal Data for any purpose other than the Business Purpose or as otherwise expressly permitted by Customer or Data

Protection Laws. The parties agree that Customer's complete and final Instructions with regard to the nature and purposes of the processing are set out in the Agreement and this DPA. Processing outside the scope of these Instructions (if any) will require prior written agreement between Customer and Panopto.

4.2. No Combination of Personal Data. Panopto is prohibited from combining Personal Data which it processes on Customer's behalf with Personal Data which it receives from or on behalf of another person or persons, or collects from its own interactions with an individual, provided that Panopto may combine Personal Data to perform the Business Purpose or as otherwise required to provide the Services.

4.3. Confidentiality. Panopto will not disclose or transfer Personal Data to any third party (other than its Personnel and authorized Sub-Processors) without the prior written consent of Customer except as required by Data Protection Laws, regulation, or public authority or as otherwise permitted by this DPA or the Agreement.

4.4. Compliance with Law Cooperation. Taking into account the nature of the Processing and the information available to Panopto, Panopto will provide Customer with such cooperation and assistance as is required by Data Protection Laws, at Customer's expense, as Customer may reasonably request to comply with Customer's obligations under Data Protection Laws, including pursuant to GPDR Articles 32 to 36, with respect to: (a) data protection impact assessments (or similar risk assessment as required under applicable Data Protection Laws) related to Customer's use of the Services to the extent the information is available to Panopto and Customer is unable to access such information necessary to perform the assessment; and/or (b) prior consultation with data protection authorities, where required and appropriate.

4.5. Security Measures. Panopto will implement and maintain reasonable and appropriate technical and organizational measures to ensure a level of security, confidentiality, availability, and integrity of Personal Data processed by Panopto in connection with the Services, taking into account the state of the art, the cost of their 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 individuals and the nature of the activities under the Agreement, including, as appropriate, the measures referred to in Article 32(1) of the GDPR. Additional details regarding the measures Panopto has taken in this regard can be found in Exhibit B attached hereto.

4.6. Legally Compelled Disclosure. If a law enforcement authority sends Panopto a demand for Personal Data (for example, through a subpoena or court order), Panopto will (a) attempt to redirect the law enforcement agency to request such Personal Data directly from Customer; and (b) promptly notify Customer of any legally binding request for disclosure of the Personal Data, unless otherwise prohibited (such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation), to allow Customer to seek a protective order or other appropriate remedy. In connection with subsection (a) above, Panopto may provide Customer's basic contact information to the law enforcement authority.

4.7. Data Subject Requests. Panopto will promptly notify Customer of (a) any Data Subject Requests received directly from a Data Subject, including individual opt-out requests, requests for access, correction, portability, and/or deletion, and all similar individual rights requests; or (b) any complaint or inquiry relating to the processing of Personal Data hereunder, including allegations that the processing infringes on any individual's or third party's rights. Panopto will not respond to any such request or complaint unless required to do so by applicable Data Protection Laws. Customer may make changes to Personal Data processed as part of the Services using features and functionality of the Services. If and to the extent that Customer is unable to respond to a Data Subject Request or other request or complaint using the features and functionality of the Services, Panopto shall, upon Customer's written request, provide Customer with commercially reasonable cooperation and assistance in fulfilling Customer's obligations to provide information about the collection, processing or usage of Personal Data in connection with a Data Subject Request at Customer's cost and solely as required by Data Protection Laws.

4.8. Infringing Instructions; Contrary Laws. Panopto will promptly inform Customer if, in its reasonable opinion, Customer's Instructions conflict with the requirements of applicable Data Protection Laws, or if Panopto foresees that it cannot comply with its contractual and legal obligations, for whatever reasons, in which case either party is entitled to suspend data processing operations governed by this DPA. Panopto will notify Customer in the event that Data Protection Laws require Processor to process Personal Data other than pursuant to the Instructions (unless prohibited from doing so by applicable law).

4.9. Breach Management and Notification. Panopto shall notify Customer without undue delay after confirmation of a Personal Data Breach. Panopto shall make reasonable efforts to identify the cause of such Personal Data Breach and will provide Customer with all breach-related information that Customer needs to demonstrate compliance with Data Protection Laws. Panopto's obligation to report or respond to a Personal Data Breach under this Section 4.9 is not and will not be construed as an acknowledgment by Panopto of any fault or liability with respect to the Personal Data Breach. Insofar as a Personal Data Breach relates to Customer, Panopto will not make any announcement about a Personal Data Breach without (a) prior written consent from Customer and (b) prior written approval by Customer

of the content, media, and timing of such notice, unless required to make a disclosure or announcement by applicable law.

4.10. Return of Personal Data. Customer may export Personal Data from the Services at any time during the Term using then-existing features and functionality of the Services. Customer is solely responsible for its data retention obligations with respect to Personal Data. On expiration or termination of the Agreement, if and to the extent Customer cannot delete and/or overwrite Personal Data stored on Panopto's systems using the then-existing features and functionality of the Services, Panopto shall delete or return all Personal Data to Customer, in accordance with Data Protection Laws, within ninety (90) days after such expiration or termination, unless Panopto is obligated by law to retain some or all of the Personal Data; provided, however, Customer shall be responsible for existing copies of Personal Data contained in files it and its users upload to Panopto's cloud-based application as permitted by the Agreement. The obligation to return or delete any Personal Data in Panopto's custody or control within the period noted above shall not apply to (a) Personal Data which Panopto has archived on its back-up systems (including, without limitation, database backups) or (b) Personal Data embedded in audit logs; backup and archival copies of Personal Data and Personal Data embedded in audit logs will remain subject to this DPA until they are destroyed in accordance with Panopto's internal data retention policies, which for backup and archival copies is no more than one (1) year after the expiration or termination of the Agreement, and for audit logs is one (1) year and one (1) day after the date of their creation. Customer will bear and pay for all costs incurred by Panopto in connection with any return or deletion of Personal Data that Customer requires Panopto to perform that is outside the scope of Panopto's customary data retention policies.

5. **Records and Audits**.

5.1. Provision of Information. To the extent required by Data Protection Laws, upon Customer's written request, Panopto shall make available to Customer the information in Panopto's control which is necessary to demonstrate Customer's compliance with Data Protection Laws.

5.2. Customer's Right to Audit. Customer may exercise its right of audit under Data Protection Laws through Panopto providing (a) a copy of Panopto's then most recent SOC 2 Type 2 report, subject to the confidentiality obligations set forth in the Agreement and (b) additional information in Panopto's possession or control to an EU Area supervisory authority when it requests or requires additional information in relation to the data processing activities carried out by Panopto under this DPA.

6. **Personnel and Sub-Processors**.

6.1. Instructions. Panopto shall require its Personnel and Sub-Processors to process Personal Data solely in accordance with the Instructions, unless otherwise required by Data Protection Laws (in which case Panopto shall notify Customer).

6.2. Confidentiality. Panopto may disclose or transfer Personal Data to its Personnel and Sub-Processors for the Business Purpose. Panopto will ensure that its Personnel and Sub-Processors are subject to confidentiality obligations that are substantially similar to those set forth in the Agreement.

6.3. Appointment of Sub-Processors. Customer hereby authorizes the appointment of, and Panopto's use of, the third-party Sub-Processors currently listed at Exhibit C (the "**Sub-Processor List**") for the processing of Personal Data for the Business Purpose. Panopto may add a third party to the Sub-Processor List, including the details of the processing and the location, by giving no less than thirty (30) days' notice to Customer (which such notice may be via email or via the Services). Customer may object to such appointment based on reasonable data protection grounds by informing Panopto in writing within fourteen (14) days of receipt of such notice. If Customer does not object within such period, that third party will be deemed an authorized Sub-Processor for the purposes of this DPA. If Customer objects in accordance with this Section 6.3, Panopto shall have the right to cure such objection through one of the following options (to be selected at Panopto's sole discretion): (a) Panopto will offer reasonable alternative(s) to provide the Services to Customer without such Sub-Processor; (b) Panopto will take reasonable steps to remove Customer's objection to, and then will proceed to use, the applicable Sub-Processor; or (c) Panopto will cease to provide or Customer cease to use (temporarily or permanently) the particular aspect of the Services that would involve the use of such Sub-Processor. If none on the above options are reasonably available to Panopto and the objection has not otherwise been resolved to each party's reasonable satisfaction within 30 days after Panopto's receipt of Customer's objection, either party may terminate the affected Order Form(s) upon written notice, and Customer will be entitled to a pro-rated refund for the prepaid fees for the Services not performed as of the date of termination. Notwithstanding the foregoing, Panopto may replace or add a Sub-Processor without prior notice to Customer if the need for the change is, in Panopto's sole discretion, urgent and necessary to provide the Services and the reason for the change is beyond Panopto's reasonable control. In such case, Panopto shall notify Customer of such Sub-Processor as soon as reasonably practicable and Customer shall retain the right to object to such Sub-Processor as set forth above.

6.4. Panopto's Obligations. Panopto shall ensure that all Sub-Processors are bound by written agreements that contain substantially similar terms as are set out in this DPA with respect to the protection of Personal Data, to the extent applicable to the nature of the services provided by such Sub-Processor. Except as otherwise set forth in the Agreement, Panopto shall be liable for the acts and omissions of its Sub-Processors to the same extent it would be liable if performing the services of each Sub-Processor directly under this DPA.

7. **Cross-Border Data Transfers**.

7.1. General Authorization to Transfer. Customer acknowledges and agrees that Panopto and its Sub-Processors may (a) provide the Services from any state, province, country, or other jurisdiction, and/or (b) transfer and process the Personal Data anywhere in the world where Panopto or its Sub-Processors maintain data processing operations. Panopto will, at all times, provide an adequate level of protection for the Personal Data processed, in accordance with the requirements of Data Protection Laws. Notwithstanding the foregoing, transfers of EU Area Personal Data are subject to the requirements set forth in Section 7.2 below.

7.2. EU Area Personal Data Transfers.

7.2.1. Order of Precedence. In the event that the Services are covered by more than one of the transfer mechanisms described below, the transfer of Personal Data will be subject to a single transfer mechanism, as applicable, and in accordance with the following order of precedence: (a) the Data Privacy Framework, as set forth in Section 7.2.2; (b) the SCCs, as set forth in Section 7.2.3; and (c) if neither (a) nor (b) is applicable, then other applicable transfer mechanisms permitted under applicable Data Protection Laws. To the extent that any substitute or additional transfer mechanisms under EU Area Law are required to transfer data to a Third Country, the parties agree to implement the same as soon as practicable and document such requirements for implementation in an attachment to this DPA.

7.2.2. Data Privacy Framework. Panopto represents that it has certified to the US Department of Commerce that it adheres to the principles set forth in the EU-US Data Privacy Framework, the UK Extension to the EU-US Data Privacy Framework, and the Swiss-US Data Privacy Framework (collectively, the "**DPF**") with regard to the processing of Personal Data received from the EEA Area (collectively, the "**DPF Principles**"). If Customer is located in the EEA Area, Panopto agrees to provide at least the same level of protection to any Personal Data as required by the DPF Principles and to promptly notify Customer if its self-certification to the DPF is withdrawn, terminated, revoked, or otherwise invalidated (in which case an alternative transfer mechanism will apply in accordance with the order of precedence in Section 7.2.1). More information about Panopto's compliance with the DPF Principles can be found at https://www.panopto.com/dpf/ (with regard to Panopto, Inc.) and at https://www.elai.io/dpf/ (with regard to Elai Inc.). To learn more about the DPF and to view Panopto's DPF certification, please visit https://www.dataprivacyframework.gov/.

7.2.3. Standard Contractual Clauses.

(a) EU Area and UK Personal Data. Transfers of EU Area Personal Data (except UK Personal Data) by Customer to Panopto in Third Countries are subject to the SCCs, and transfers of UK Personal Data by Customer to Panopto in Third Countries are subject to the SCCs as amended by the UK Addendum, specifically Module Two (Controller to Processor) when Customer is a Controller and Panopto is processing Personal Data for Customer as a Processor, and Module Three (Processor to Processor) when Customer is a Processor and Panopto is processing Personal Data on behalf of Customer as a Sub-Processor. For each module, where applicable, the following applies:

(i) The optional docking clause in Clause 7 does not apply.

(ii) In Clause 9, Option 2 applies, and the minimum time period for prior notice of sub-processor changes shall be as set forth in Section 6.3 of this DPA.

(iii) In Clause 11, the optional language does not apply.

(iv) All square brackets in Clause 13 are hereby removed.

(v) In Clause 17, the SCCs will be governed by Ireland law.

(vi) In Clause 18(b), disputes will be resolved before the courts of Ireland;

(vii) Exhibit A to this DPA contains the information required in Annex I and Annex II of the SCCs.

(viii) Exhibit B to this DPA contains the information required in Annex III of the SCCs.

(ix) Exhibit C to this DPA contains the information required in Annex IV of the SCCs.

(x) By entering into this DPA, the parties are deemed to have signed the applicable SCCs

incorporated herein, including their Annexes.

(b) Swiss Personal Data. For transfers of Personal Data by Customer to Panopto that are subject to the FADP, the SCCs shall apply, with the following modifications:

(i) References to the GDPR in the SCCs are understood to be as references to the FADP insofar as the data transfers are subject exclusively to the FADP and not to the GDPR. References to the GDPR in the SCCs are understood to be as references to the FADP and the GDPR insofar as the data transfers are subject to both the FADP and the GDPR.

(ii) The term "member state" 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.

(iii) References to personal data in the SCCs also refer to data about identifiable legal entities until the entry into force of revisions to the FADP that eliminate this broader scope.

(c) Supplementary Measures. In respect of any transfer of Personal Data to a Third Country, the following supplementary measures shall apply:

(i) As of the date of this DPA, Panopto has not received any formal legal requests from any government intelligence or security service/agencies in the country to which the Personal Data is being exported, for access to (or for copies of) Personal Data ("Government Agency Requests").

(ii) If, after the date of this DPA, Panopto receives any Government Agency Requests, it shall attempt to redirect the law enforcement or government agency to request the applicable Personal Data directly from Customer. As part of this effort, Panopto may provide Customer's basic contact information to the government agency. If compelled to disclose Personal Data to a law enforcement or government agency, Panopto shall give Customer reasonable notice of the demand and reasonably cooperate to allow Customer to seek a protective order or other appropriate remedy unless Panopto is legally prohibited from doing so. Panopto shall not voluntarily disclose Personal Data to any law enforcement or government agency. Customer and Panopto shall (as soon as reasonably practicable) discuss and determine whether all or any transfers of Personal Data pursuant to this DPA should be suspended in the light of the such Government Agency Requests.

(iii) Customer and Panopto will meet as needed to consider whether: (1) the protection afforded by the laws of the country of Customer to Data Subjects whose Personal Data is being transferred is sufficient to provide broadly equivalent protection to that afforded in the applicable EU Area; (2) additional measures are reasonably necessary to enable the transfer to be compliant with the Data Protection Laws; and (3) It is still appropriate for Personal Data to be transferred to Panopto, taking into account all relevant information available to the parties, together with guidance provided by the supervisory authorities.

(iv) If Data Protection Laws require Customer to execute the SCCs applicable to a particular transfer of Personal Data to Panopto as a separate agreement, Panopto shall, on written request of Customer, promptly execute such SCCs incorporating such amendments as may reasonably be required by Customer to reflect the applicable appendices and annexes, the details of the transfer and the requirements of the relevant Data Protection Laws.

(v) If either (1) any of the means of legitimizing transfers of Personal Data outside of the applicable EU Area set forth in this DPA cease to be valid or (2) any supervisory authority requires transfers of Personal Data pursuant to those means to be suspended, then Panopto may by notice to Customer, with effect from the date set out in such notice, amend or put in place alternative arrangements in respect of such transfers, as required by Data Protection Laws.

8. **Panopto's Liability**. Panopto's entire liability arising out of or relating to this DPA (including the SCCs), whether in contract, tort, or under any other theory of liability, is subject to the applicable exclusions and limitations of liability clauses set forth in the Agreement. For the avoidance of doubt, Panopto's total liability for all claims from Customer and all of its users arising out of or related to the Agreement or this DPA will apply in aggregate for all claims under both the Agreement and this DPA. Nothing in this DPA will limit Panopto's liability with respect to any liability or loss which may not be limited under Data Protection Laws.

9. **Miscellaneous.**

9.1. Governing Law. This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by Data Protection Laws.

9.2. No Third Party Beneficiaries. A person who is not a party to this DPA will not have any rights under this DPA (including under the Contracts (Rights of Third Parties) Act 1999) to enforce any term of this DPA. No one other than a party to this DPA (and their respective successors and permitted assignees) shall have any right to enforce any of its terms, unless otherwise required by Data Protection Laws.

9.3. Severability. The provisions of this DPA are severable. If any phrase, clause, or provision is invalid or unenforceable, in whole or in part, such invalidity or unenforceability shall affect only such phrase, clause, or provision, and the rest of the DPA shall remain in full force and effect.

9.4. Order of Precedence. Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Agreement, this DPA shall prevail to the extent of that conflict so far as the subject matter concerns the processing of Personal Data. In the event of any conflict or inconsistency between the terms of this DPA and the terms the SCCs, then, only insofar as the SCCs apply, the SCCs shall prevail.

9.5. Entire Agreement. This DPA constitutes and embodies the entire agreement and understanding between the parties with respect to the subject matter hereof and supersedes all prior or contemporaneous written, electronic or oral communications, representations, agreements or understandings between the parties with respect thereto. Other than in respect of statements made fraudulently, no other representations or terms will apply or form part of this DPA. This DPA is without prejudice to the rights and obligations of the parties under the Agreement which will continue to have full force and effect. Panopto may modify the terms contained in this DPA at any time by posting the applicable updated version on Panopto's website at https://www.panopto.com/data-processing-agreement/ or by otherwise notifying Customer as described in the Agreement. The modified terms will become effective upon posting or, if Panopto notifies Customer as described in the Agreement, as stated in the notice provided. By continuing to use the Services after the effective date of any such modifications, Customer agrees to be bound by the modified terms. It is also Customer's responsibility to check the Panopto website regularly for any such modifications.

EXHIBIT A

A. LIST OF PARTIES

Data exporter(s):

Name: The Customer that is a party to the DPA to which this Exhibit A is attached.

Address: As set forth in the relevant Agreement.

Contact person's name, position and contact details: As set forth in the relevant Agreement.

Activities relevant to the data transferred under these Clauses:

Data exporter is an entity that has subscribed to data importer's software-as-a-service and related services, as more fully described in the Agreement and the applicable Order Form(s).

Role (controller/processor): Controller or Processor, as the case may be.

Data importer(s):

Name: The Panopto entity that is a party to the DPA to which this Exhibit A is attached.

Address: As set forth in the relevant Agreement.

Contact person's name, position and contact details: Data Protection Officer, data-protection@panopto.com.

Activities relevant to the data transferred under these Clauses:

Data importer is a company providing software-as-a-service and related services, which generally speaking is (1) for the Panopto Services, software that provides recording, screencasting, video streaming, and video content management and (2) for the Elai Services, an AI-powered text-to-video platform that provides interactive playback, creator tools, and avatar-based learning, as more fully described in the Agreement and the applicable Order Form(s).

Role (controller/processor): Processor or Sub-Processor, as the case may be.

B. DESCRIPTION OF TRANSFER

1. Categories of data subjects whose personal data is transferred:

- Data exporter's Primary Administrator and Billing Contact (if different from Administrator)
- Data exporter's Authorized Users who access data importer's Services
- Viewers of data exporter's uploaded Customer Content
- Data Subjects depicted, referenced, or recorded by data exporter within data exporter's uploaded Customer Content
- Other Data Subjects as defined by data exporter in its sole discretion

2. Categories of personal data transferred:

Data Exporter Personal Data:

a. Name
b. Email address
c. Mailing and billing address, phone and fax number
d. Billing and accounting information, including payment details

Primary administrator, billing contact, Authorized User, and viewer Personal Data:

a. Name
b. Email Address
c. Organization, Employer, or Relation to data exporter
d. IP address

e. Access, usage, and event details

f. Date and time stamps

g. Actions taken

h. Operating system, browser, and device type

i. Performance metrics of platform

j. Referring and exit pages

Customer Content:

a. Personal Data and Sensitive Personal Data, as determined by the data exporter in its sole discretion, which may include photographic, video, and audio recordings, physical characteristics or descriptions, and likenesses of, or references to, Data Subjects.

b. Other Personal Data or Sensitive Personal Data, as defined by the data exporter in its sole discretion

3. Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:

   Sensitive data may be transferred by the data exporter in its sole discretion

4. The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):

   The data is transferred on a continuous basis as users interact with the Services, including uploading and generating Customer Content and collected usage data.

5. Nature of the processing:

   The nature of the processing of the Personal Data is as described in the Agreement and applicable Order Form(s) and generally includes the collection, storage, and processing of Personal Data to provide, maintain, and enhance the Services, including customer support, service monitoring, and content generation.

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

   The purpose for the collection, processing, and use of the Personal Data by data importer is to provide the Services as described in the Agreement and applicable Order Form(s).

7. The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:

   The duration of the processing will expire upon the termination of the Agreement or as soon thereafter as is reasonably possible. Data importer will not retain Personal Data any longer than is necessary to accomplish the purposes of the processing.

8. For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:

   The subject matter, nature, and duration of the processing are more fully described in the Agreement, the DPA, and the Order Form(s). Transfers to Sub-Processors will occur on a one-off basis as needed to enable the applicable Sub-Processor to provide the applicable services.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13: For matters related to data transfers pursuant to the GDPR:

1. Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer shall act as competent supervisory authority.

2. Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established shall act as competent supervisory authority.

3. Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located shall act as competent supervisory authority.

For matters related to data transfers pursuant to the UK GDPR: Where the transfer is subject exclusively to the UK GDPR and not the GDPR, the supervisory authority is the UK Information Commissioner's Office. Where the transfer is subject to both the UK GDPR and the GDPR, the supervisory authority is the UK Information Commissioner's Office insofar as the transfer is governed by the UK GDPR, and the supervisory authority as set forth above insofar as the transfer is governed by the GDPR.

For matters related to data transfers pursuant to the FADP: Where the transfer is subject exclusively to the FADP and not the GDPR, the supervisory authority is the Federal Data Protection and Information Commissioner of Switzerland. Where the transfer is subject to both the FADP and the GDPR, the supervisory authority is the Swiss Federal Data Protection and Information Commissioner insofar as the transfer is governed by the FADP, and the supervisory authority as set forth above insofar as the transfer is governed by the GDPR.

EXHIBIT B

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Panopto maintains an information security program that is subject to audit by an independent third party and that includes administrative, technical, and physical safeguards to ensure the confidentiality, integrity, and availability of Personal Data. Such safeguards are commensurate with the sensitivity of the information and no less stringent than required by applicable Data Protection Laws. Panopto's security controls include without limitation:

- Maintaining a risk assessment process, conducted at least annually and whenever there is a material change in Panopto's business practices, to identify, assess, and mitigate internal and external risks to Personal Data and information systems
- Ensuring that vendors and service providers that access Personal Data or information systems maintain appropriate security controls
- Establishing, maintaining, and testing incident response procedures
- Providing security awareness and role-specific security training to employees and contractors
- Limiting access to Personal Data to authorized individuals who need access to perform their duties
- Performing background checks on all employees and contractors
- Monitoring systems to prevent, detect, and respond to unauthorized use of or access to Personal Data
- Testing changes for information systems to ensure that the security of such systems and associated environments are not compromised
- Encrypting all Personal Data in transit and at rest
- Performing regular vulnerability scans and penetration tests of systems that contain Personal Data
- Maintaining malicious software protection that is configured to receive regular updates
- Ensuring physical security of all premises in which Personal Data is processed, stored, and/or transmitted
- Disposing media containing Personal Data using methods that prevent it from being reassembled, read, or reconstituted

For transfers to Sub-Processors, also describe the specific technical and organisational measures to be taken by the Sub-Processor to be able to provide assistance to the controller and, for transfers from a processor to a Sub-Processor, to the data exporter

Panopto conducts reasonable due diligence and security assessments of Sub-Processors and enters into agreements with Sub-Processors that contain provisions similar to or more stringent than those provided for in this DPA. Panopto will work directly with Sub-Processors, as necessary, to provide assistance to data exporter.

Exhibit C

Sub-Processor List

Sub-Processors for Panopto Services		
Name of Sub-Processor	**Nature of Processing Activities**	**Location of Processing**
Panopto Affiliates*	Platform interface, customer support services, and website services	Panopto, Inc.: United States Panopto EMEA Limited: United Kingdom Panopto ANZ Pty Ltd: Australia Panopto Asia Pacific Limited: Hong Kong Panopto Asia Pte Ltd: Singapore Elai Inc.: United States
Amazon Web Services	Web hosting, AI Search and translation services	United States, Canada, Ireland, Australia, Japan or Singapore, as selected by Customer and/or as set forth in the Agreement
All Lines Technology**	24x7 customer support services	United States
Cielo24**	Captioning services	United States
Verbit**	Captioning services and audio descriptions	United States
3Play Media**	Captioning services and audio descriptions	United States
Google Analytics**	Business operations	Any country in which Google maintains facilities, as set forth at: https://www.google.com/about/datacenters/locations/
Salesforce.com	Business operations	United States
Marketo	Business operations	United States
Pendo.io	Business operations	United States
ChurnZero	Business operations	United States
Luzmo**	Data analytics services	United States, Canada, Ireland, Australia, Japan or Singapore, as selected by Customer and/or as set forth in the Agreement
Omni.ai**	Translation and transcription services	United States, Canada, Ireland, Australia, Japan or Singapore, as selected by Customer and/or as set forth in the Agreement
Speechmatics**	Transcription services	United States, Canada, Ireland, Australia, Japan or Singapore, as selected by Customer and/or as set forth in the Agreement

*Elai Inc. is only a Sub-Processor if Customer purchases Elai as an add-on service. The other Panopto entities are Sub-Processors only to the extent that Personal Data must be shared with them in order for the contracting Panopto entity to provide the Services to Customer.

**Asterisks indicate Sub-Processors only to the extent that Customer has chosen that specific Panopto add-on service or support package pursuant to the applicable Order Form(s). In the case of Google Analytics, it is only a Sub-Processor if and to the extent Customer has opted in to using Google Analytics within the Services (Google Analytics is turned off by default, so it not a Sub-Processor unless Customer is utilizing the Google Analytics integration within the Services for its own analytics purposes).

Sub-Processors for Elai Services		
Name of Sub-Processor	**Nature of Processing Activities**	**Location of Processing**
Elai Affiliates*	Platform interface, customer support services, and website services	Panopto, Inc.: United States Panopto EMEA Limited: United Kingdom Panopto ANZ Pty Ltd: Australia Panopto Asia Pacific Limited: Hong Kong Panopto Asia Pte Ltd: Singapore
Amazon Web Services	Web hosting services and AI research and development	United States or Germany, as selected by Customer and/or as set forth in the Agreement
Microsoft Azure	Voice editor	United States
ElevenLabs	Voice editor	United States
Assembly AI	Voice editor	United States
Google	Voice editor	United States
Lunaweb	File converter	United States
Mixpanel	Analytics	United States
Pendo.io	Analytics	United States
Contentsquare	Analytics	France
Pipio	Avatars library	United States
HeyGen	Avatars library	United States
Moderation api	Content moderation	Denmark
Sinch Mailgun	Business operations	United States

*The Panopto entities are Sub-Processors only to the extent that Personal Data must be shared with them in order for Elai to provide the Services to Customer or if Customer purchases Panopto as an add-on service.