

PANOPTO DATA PROCESSING AGREEMENT

Last Updated: July 30, 2024

This Panopto Data Processing Agreement (this “**DPA**”) between Customer and Panopto establishes the parties’ respective responsibilities under Data Protection Laws (as defined below) with respect to Personal Data to be processed by Panopto as a Processor pursuant to the Technology Services Agreement or similar 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 an Order Form or other document incorporating the Agreement that references 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 the Panopto entity that is a party to the Agreement with Customer (i.e., either Panopto, Inc. or one of its Affiliates).
- 1.8. “**Personal Data**” means any data which (i) qualifies as “Personal Data”, “Personal Information”, “Personally Identifiable Information” or any substantially similar term under applicable Data Protection Laws and (ii) 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 the 2021 EU SCCs and/or the 2021 EU SCCs as amended by the UK Addendum or any applicable successor clauses to either of the foregoing. “**2021 EU SCCS**” means the standard contractual clauses for the transfer of European Area Personal Data to Third Countries as adopted by the European Commission or any successor clauses thereto.
- 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. **“UK Addendum”** means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses as issued by the UK Information Commissioner under s119A(1) of the UK Data Protection Act 2018, Version B1.0, in force 21 March 2022, or such alternative as may be approved by the UK Information Commissioner from time to time.
- 1.16. 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, 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 Annex I to Exhibit 1 attached hereto, which is hereby incorporated by reference.
- 2.2. **Role of the Parties.** As between Customer and Panopto, Customer is the Data Controller (as defined by Data Protection Laws) and Business (collectively, **“Controller”**) of the Personal Data and Panopto is the Data Processor (as defined by Data Protection Laws) and Service Provider (collectively, **“Processor”**) for the Personal Data processed by Panopto in connection with Customer’s access to and use of the Services.
- 2.3. **Compliance with Data Protection Laws.** Each Party will comply with its obligations under Data Protection Laws in connection with the processing of Personal Data. In connection with its access to and use of the Services, Controller shall process Personal Data within the Services and provide Processor with instructions in accordance with Data Protection Laws.

3. Controller’s Obligations.

- 3.1. **General.** Controller represents and warrants to Processor that (a) Controller will remain duly and effectively authorized to give the Instructions (defined below) set out in the Agreement, this DPA, or as Controller otherwise provides; and (b) Controller retains responsibility for responding, and Controller 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.** Controller is solely responsible for the accuracy, quality, and legal compliance relating to the Personal Data. Controller’s use of the Services will not violate the privacy, data protection, or other rights of any third party. Processor has no control over the nature, scope, or origin of, or the means by which Controller acquires, Personal Data.
- 3.3. **Notice and Choice.** Controller is solely responsible for providing its end users with appropriate notice regarding its processing activities. Controller 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 Controller or its end users to Processor in connection with the Services. Controller also retains responsibility for the creation, maintenance, and testing of any backups for Customer Content.

4. Processor’s Obligations.

- 4.1. **Instructions.** Controller instructs Processor (and authorizes Processor 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”**). Processor 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 Controller or Data Protection Laws. The parties agree that Controller’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 Controller and Processor.
- 4.2. **No Combination of Personal Data.** Processor is prohibited from combining Personal Data which Processor processes on Controller’s behalf with Personal Data which Processor receives from or on behalf of another person or persons, or collects from its own interactions with an individual, provided that Processor may combine Personal Data to

perform the Business Purpose or as otherwise required to provide the Services.

- 4.3. Confidentiality. Processor will not disclose or transfer Personal Data to any third party (other than its Personnel) without the prior written consent of Controller 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 Processor, Processor will provide Controller with such cooperation and assistance as is required by Data Protection Laws, at Controller's expense, as Controller may reasonably request to comply with Controller's obligations under Data Protection Laws, including pursuant to GDPR 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 Controller's use of the Services to the extent the information is available to Processor and Controller 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. Processor 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 Processor 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 Processor has taken in this regard can be found in Annex II to Exhibit 1 attached hereto.
- 4.6. Legally Compelled Disclosure. If a law enforcement authority sends Processor a demand for Personal Data (for example, through a subpoena or court order), Processor will (a) attempt to redirect the law enforcement agency to request such Personal Data directly from Controller; and (b) promptly notify Controller 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 Controller to seek a protective order or other appropriate remedy. In connection with subsection (a) above Processor may provide Controller's basic contact information to the law enforcement authority.
- 4.7. Data Subject Requests. Processor will promptly notify Controller 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. Processor will not respond to any such request or complaint unless required to do so by applicable Data Protection Laws. Controller 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 Controller is unable to respond to a Data Subject Request or other request or complaint using the features and functionality of the Services, Processor shall, upon Controller's written request, provide Controller with commercially reasonable cooperation and assistance in fulfilling Controller's obligations to provide information about the collection, processing or usage of Personal Data in connection with a Data Subject Request at Controller's cost and solely as required by Data Protection Laws.
- 4.8. Infringing Instructions; Contrary Laws. Processor will promptly inform Controller if, in its reasonable opinion, Controller's Instructions conflict with the requirements of applicable Data Protection Laws, or if Processor 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. Processor will notify Controller 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. Processor shall notify Controller without undue delay after confirmation of a Personal Data Breach. Processor shall make reasonable efforts to identify the cause of such Personal Data Breach and will provide Controller with all breach-related information that Controller needs to demonstrate compliance with Data Protection Laws. Processor'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 Processor of any fault or liability with respect to the Personal Data Breach. Insofar as a Personal Data Breach relates to Controller, Processor will not make any announcement about a Personal Data Breach (a "**Breach Notice**") without (a) prior written consent from Controller and (b) prior written approval by Controller of the content, media, and timing of the Breach Notice, unless required to make a disclosure or announcement by applicable law.
- 4.10. Return of Personal Data. Controller 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 Controller cannot delete and/or overwrite Personal Data stored on Processor's systems using the then-existing features and functionality of the Services, Processor shall delete or return all Personal Data to Controller, in accordance with Data Protection Laws, within ninety (90) days after such expiration or termination, unless Processor is obligated by law to retain some or all of the Personal Data; provided, however, Controller shall be responsible for existing copies of Personal Data contained in files Controller and its users upload to Processor's cloud-based application as permitted by the Agreement. The obligation to return or delete any Personal Data in Processor's custody or control within the period noted above shall not apply to (a) Personal Data which Processor 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 Processor'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. Controller will bear and pay for all costs incurred by Processor in connection with any return or deletion of Personal Data that Controller requires Processor to perform that is outside the scope of Processor'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, Processor shall make available to Controller the information in Processor's control which is necessary to demonstrate Controller's compliance with Data Protection Laws.
- 5.2. Controller's Right to Audit. Controller may exercise its right of audit under Data Protection Laws through Processor providing (a) a copy of Processor's then most recent SOC 2 Type 2 report, subject to the confidentiality obligations set forth in the Agreement and (b) additional information in Processor'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 Processor under this DPA.

6. Personnel and Sub-Processors.

- 6.1. Instructions. Processor shall require Processor's Personnel and Sub-Processors to process Personal Data solely in accordance with the Instructions, unless otherwise required by Data Protection Laws (in which case Processor shall notify Controller).
- 6.2. Confidentiality. Processor may disclose or transfer Personal Data to Processor's Personnel and Sub-Processors for the Business Purpose. Processor 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. Controller hereby authorizes the appointment of, and Processor's use of, the third-party Sub-Processors currently listed at Exhibit 3 (the "**Sub-Processor List**") for the processing of Personal Data for the Business Purpose. Processor may, by giving no less than thirty (30) days' notice to Controller (which such notice may be via email or via the Services), add or make changes to the Sub-Processor List, and Processor will make such updated version of the Sub-Processor List, including the details of the processing and the location, available to Controller. If Controller objects to the appointment of any new Sub-Processor on reasonable data protection grounds within fourteen (14) days of such notice, Processor shall have the right to cure any objection that Controller has through one of the following options (to be selected at Processor's sole discretion): (a) Processor will offer reasonable alternative(s) to provide its services without such Sub-Processor; (b) Processor will take reasonable steps to remove Controller's objection to, and will proceed to use, the applicable Sub-Processor with regard to the Personal Data; or (c) Processor may cease to provide or Controller cease to use (temporarily or permanently) the particular aspect of the Services that would involve the use of such Sub-Processor. If none of the above options are reasonably available to Processor and the objection has not been resolved to each party's reasonable satisfaction within 30 days after Processor's receipt of Controller's objection, either Party may terminate the affected Order Form(s) and Controller will be entitled to a pro-rata refund for the prepaid fees for the Services not performed as of the date of termination. Notwithstanding the foregoing, Processor may replace a Sub-Processor without prior notice to Controller if the need for the change is, in Processor's sole discretion, urgent and necessary to provide the Processor's services and the reason for the change is beyond the Processor's reasonable control. In such case, Processor shall notify Controller of such replacement as soon as reasonably practicable and Controller shall retain the right to object to the replacement Sub-Processor as set forth above.
- 6.4. Processor's Obligations. Processor 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, Processor shall be liable for the acts and omissions of its Sub-Processors to the same extent Processor 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 2021 EU SCCs or the 2021 EU SCCs as modified by the UK Addendum, 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/>. 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 Personal Data. Transfers of EU Area Personal Data (except UK Personal Data) by Controller to Processor in Third Countries are subject to the 2021 EU SCCs, *Module Two* (Controller to Processor) attached hereto and incorporated by reference as Exhibit 1 . **For the sake of clarity, if and to the extent the 2021 EU SCCs apply, signatures of assent of Customer and Panopto to the Agreement will be deemed signatures to the 2021 EU SCCs.** To the extent that any substitute or additional appropriate safeguards or mechanisms under any EU Area Law are required to transfer data to a Third Country, the parties agree to implement the same as soon as is reasonably practicable and document such requirements for implementation in an attachment to this DPA.
- (b) Swiss Personal Data. For transfers of Personal Data that are subject to the FADP, the 2021 EU SCCs shall apply, with the following differences to the extent required by the FADP:
 - (i) References to the GDPR in the 2021 EU 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 2021 EU SCCs are understood to be as references to both the FADP and/or the Revised FADP (as applicable) 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 2021 EU SCCs;
 - (iii) References to personal data in the 2021 EU SCCs also refer to data about identifiable legal entities until the entry into force of revisions to the FADP that eliminate this broader scope; and
 - (iv) Under Annex I.C of the 2021 EU SCCs (Competent Supervisory Authority), (1) where the transfer is subject exclusively to the FADP and not the GDPR, the supervisory authority is the

Swiss Federal Data Protection and Information Commissioner; and (2) 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 in Annex I.C insofar as the transfer is governed by the GDPR.

- (c) **UK Personal Data.** Transfers of UK Personal Data by Customer to Panopto in Third Countries are subject to the 2021 EU SCCs as modified by the UK Addendum attached hereto and incorporated by reference as Exhibit 2. **For the sake of clarity, if and to the extent that the UK Addendum applies, signatures of assent of Customer and Panopto to the Agreement will be deemed signatures to the UK Addendum.**
 - (d) The following terms will apply to the 2021 EU SCCs and the 2021 EU SCCs as modified by the UK Addendum, whether used pursuant to this Section 7.2.1 or Section 7.2.2 below:
 - (i) On request by a Data Subject, Customer may make a copy of the 2021 EU SCCs available to the Data Subject in accordance with Clause 8.3 of the 2021 EU SCCs. Customer shall not make the entirety of this DPA available, but a copy of the 2021 EU SCCs only, and Customer shall use commercially reasonable efforts to consult with Panopto in order to redact the 2021 EU SCCs to the extent necessary to protect Panopto's business secrets or other Confidential Information prior to sharing the 2021 EU SCCs with the Data Subject. The parties shall use good faith efforts to coordinate a response to the Data Subject regarding the reasons for the redactions, to the extent reasonably practicable without revealing the redacted information.
 - (ii) Panopto will provide assistance to Customer to erase or rectify inaccurate Personal Data in accordance with Clause 8.4 of the 2021 EU SCCs by providing appropriate technical and organizational measures where possible through the Services and/or as outlined in the Documentation.
 - (iii) for purposes of Clause 8.5 of the 2021 EU SCCs, Panopto will (1) comply with its obligations to return or destroy all Personal Data as specified in Section 4.10 (Return of Personal Data) of this DPA and (2) provide certification of such destruction on upon Customer's written request therefor.
 - (iv) Customer's right of audit under clauses 8.9 of the 2021 EU SCCs may be exercised as specified in Section 5 (Records and Audits) of this DPA.
 - (v) Customer's rights regarding Panopto's Sub-Processors under clause 9(a) of the 2021 EU SCCs are subject to Section 6 (Personnel and Sub-Processors) of this DPA. The parties agree that copies of the Sub-Processor agreements that Panopto must provide to Customer pursuant to clause 9(c) of the 2021 EU SCCs may have commercial information, or clauses unrelated to the 2021 EU SCCs or their equivalent, removed by Panopto beforehand, and that such copies will be provided only upon written request by Customer.
8. **Processor's Liability.** Processor'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, Processor's total liability for all claims from Controller 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 Processor'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 1

STANDARD CONTRACTUAL CLAUSES

Module Two: Transfer Controller to Processor

For EU Area Personal Data transfers (excluding UK Personal Data)

SECTION I

Clause 1

Purpose and scope

- (a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ⁽¹⁾ for the transfer of data to a third country.
- (b) The Parties:
 - (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and
 - (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed Annex I.A (hereinafter each 'data importer') have agreed to these standard contractual clauses (hereinafter: 'Clauses').
- (c) These Clauses apply with respect to the transfer of personal data as specified in Annex 1.B.
- (d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

- (a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.
- (b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

- (a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
 - (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
 - (ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

¹ Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/ED (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

- (iii) Clause 9(a), (c), (d) and (e);
- (iv) Clause 12(a), (d) and (f);
- (v) Clause 13;
- (vi) Clause 15.1(c), (d) and (e);
- (vii) Clause 16(e);
- (viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

- (a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
- (b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
- (c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking clause

- (a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
- (b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
- (c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

- (a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
- (b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

- (a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
- (b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- (c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.
- (d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or

trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union ⁽⁴⁾ (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

- (i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- (ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
- (iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- (iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

- (a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
- (b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.
- (c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.
- (d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
- (e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

- (a) **GENERAL WRITTEN AUTHORISATION** The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least thirty (30) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.
- (b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. ⁽⁸⁾ The

⁴ The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

⁸ This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance

Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

- (c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
- (d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.
- (e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

- (a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.
- (b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
- (c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

- (a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.
- (b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
- (c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
 - (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
 - (ii) refer the dispute to the competent courts within the meaning of Clause 18.
- (d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
- (e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
- (f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

- (a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
- (b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any

with Clause 7.

material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

- (c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.
- (d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
- (e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
- (f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.
- (g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

- (a) 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 is the EU Member State in which the data exporter is established and shall act as competent supervisory authority.

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, as indicated in Annex I.C, shall act as competent supervisory authority.

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, as indicated in Annex I.C, shall act as competent supervisory authority.

- (b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

- (a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
- (b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
 - (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of

processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

- (ii) the laws and practices of the third country of destination— including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ⁽¹²⁾;
 - (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
- (c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
 - (d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
 - (e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).
 - (f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

- (a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
 - (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
 - (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
- (b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of

¹² As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

- (c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).
- (d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
- (e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

- (a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).
- (b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.
- (c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

- (a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
- (b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
- (c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
 - (i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
 - (ii) the data importer is in substantial or persistent breach of these Clauses; or
 - (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

- (d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required

under that local law.

- (e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be (a) the law of the EU Member State in which the data exporter is established; or (b) if the data exporter is not established in any EU Member State, the law of Germany.

Clause 18

Choice of forum and jurisdiction

- (a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- (b) The Parties agree that those shall be the courts of Germany.
- (c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
- (d) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

1. **Name:** The Customer that is a party to the DPA to which this Exhibit 1 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

Data importer(s):

1. **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 software that provides recording, screencasting, video streaming, and video content management, to its customers, as more fully described in the Agreement and the applicable Order Form(s).

Role (controller/processor): Processor

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 Processor'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, and Authorized User Personal Data:

- a. Name
- b. Email Address
- c. Organization, Employer, or Relation to data exporter

Viewer (licensed, or non-licensed) Personal Data may include:

- a. IP address

- b. Access, usage, and event details
- c. Location, date, and time stamps
- d. Actions taken
- e. Operating system, browser, and device type
- f. Performance metrics of platform
- g. Referring and exit pages

Error reports and usage analytics may include:

- a. IP address
- b. Access, usage, and event details
- c. Location, date, and time stamps
- d. Actions taken
- e. Operating system, browser, and device type
- f. Performance metrics of platform

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 one-off basis as needed when data importer's personnel perform updates and upgrades to the servers on which the Services are hosted and when data importer's personnel provide technical support to data exporter and/or data exporter's users of the Services.
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 recording, screen casting, video streaming, and video content management.
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 (for example, and not by way of limitation, providing captioning services to the extent data exporter has ordered such services pursuant to an ordering document).

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.
4. For matters related to data transfers pursuant to the **FADP**: The Federal Data Protection and Information Commissioner of Switzerland

■

ANNEX II

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 2
UK Addendum
International Data Transfer Addendum to the EU Commission Standard Contractual Clauses
 (Version B1.0, in force 21 March 2022)

This Addendum has been issued by the UK Information Commissioner for Parties making Restricted Transfers. The UK Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start date	This Addendum will take effect on the DPA Effective Date.	
The parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Parties' details	See Annex I.A to Exhibit 1	See Annex I.A to Exhibit 1
Key Contact	See Annex I.A to Exhibit 1	See Annex I.A to Exhibit 1

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	The version of the Approved EU SCCs which this Addendum is appended to is as set forth in Exhibit 1 of the 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 Addendum is set out in:

Annex 1A: List of parties:	As per Table 1 above.
Annex 1B: Description of transfer:	See Annex I to Exhibit 1 of the DPA.
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:	See Annex II to Exhibit 1 of the DPA.
Annex III: List of Sub-Processors (Modules 2 and 3 only):	See Exhibit 3 of the 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: <input type="checkbox"/> Importer <input type="checkbox"/> Exporter <input checked="" type="checkbox"/> Neither party
--	--

Part 2: Mandatory Clauses

Entering into this Addendum

- Each party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other party also agreeing to be bound by this Addendum.
- Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the parties, for the purpose of making Restricted Transfers, the parties may enter into this Addendum in any way that makes them legally binding on the parties

and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the parties' obligation to provide the Appropriate Safeguards.
5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.
6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.
7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.
8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.
11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:
 - a. Together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;
 - b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and
 - c. This Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.
13. Unless the parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.
14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.
15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:
 - a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;
 - b. In Clause 2, delete the words:

"and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";
 - c. Clause 6 (Description of the transfer(s)) is replaced with:

"The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";
 - d. Clause 8.7(i) of Module 1 is replaced with:

"it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";
 - e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

"the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"
 - f. References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;
 - g. References to Regulation (EU) 2018/1725 are removed;
 - h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";
 - i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";
 - j. Clause 13(a) and Part C of Annex I are not used;

- k. The “competent supervisory authority” and “supervisory authority” are both replaced with the “Information Commissioner”;
- l. In Clause 16(e), subsection (i) is replaced with:
 “the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply.”;
- m. Clause 17 is replaced with:
 “These Clauses are governed by the laws of England and Wales.”;
- n. Clause 18 is replaced with:
 “Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts.”; and
- o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

- 16. The parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.
- 17. If the parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.
- 18. From time to time, the ICO may issue a revised Approved Addendum which:
 - a. Makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
 - b. Reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

- 19. If the ICO issues a revised Approved Addendum under Section 18, if any party selected in Table 4 “Ending the Addendum when the Approved Addendum changes”, will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:
 - a. its direct costs of performing its obligations under the Addendum; and/or
 - b. its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other party before the start date of the revised Approved Addendum.

- 20. The parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

Alternative Part 2 Mandatory Clauses:

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 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.
--------------------------	---

Exhibit 3

Sub-Processor List

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: Singapore Panopto Asia Pte Ltd: Hong Kong
Amazon Web Services	Web hosting 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	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
Tableau	Business operations	United States
Marketo	Business operations	United States
Pendo.io	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

*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 if Customer is located in the European Union, so it not a Sub-Processor unless Customer is utilizing the Google Analytics integration within the Services for its own analytics purposes).