Data Processing Agreement

USING THIS DPA

This DPA has 2 parts: (1) the Key Terms on this Cover Page and (2) the Common Paper DPA Standard Terms Version 1.1 posted at http://commonpaper.com/standards/data-processing-agreement/1.1/ ("**DPA Standard Terms**"), which is incorporated by reference. If there is any inconsistency between the parts of the DPA, the Cover Page will control over the DPA Standard Terms. Capitalized and **highlighted** words have the meanings given on the Cover Page. However, if the Cover Page omits or does not define a highlighted word, the default meaning will be "none" or "not applicable" and the correlating clause, sentence, or section does not apply to this DPA. All other capitalized words have the meanings given in the DPA Standard Terms or the **Agreement**. A copy of the DPA Standard Terms is attached for convenience only.

Key Terms

The key legal terms of the DPA are as follows:

Agreement	This DPA supplements the Mindsmith Terms of Service at https://www.mindsmith.ai/terms-conditions accepted by Customer or, where the parties have signed one, the Master Services Agreement or Order Form between Customer and Mindsmith Learning, Inc. ("Provider" or "Mindsmith").
Approved Subprocessors	[x] List of Subprocessors, with country of location and Processing task, available at https://trust.mindsmith.ai (Subprocessors section).
Provider Security Contact	security@mindsmith.ai Mindsmith Learning, Inc., 3400 N. Ashton Blvd., Ste. 410, Lehi, UT 84043, United States
Security Policy	[x] Security Policy available at https://trust.mindsmith.ai (Network Security Policy and related security documentation). [x] Provider will maintain annually updated reports or annual certifications of compliance with the following: [ ] ISO 27001 [ ] SOC 2 Type I [x] SOC 2 Type II [ ] HIPAA [x] Penetration testing [ ] PCI Level 1 [ ] PCI Level 2 [ ] FedRAMP Authorized
Changes to the Agreement	
Service Provider Relationship	[x] To the extent California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq ("CCPA") applies, the parties acknowledge and agree that Provider is a service provider and is receiving Personal Data from Customer to provide the Service as agreed in the Agreement and detailed below (see Nature and Purpose of Processing), which constitutes a limited and specified business purpose. Provider will not sell or share any Personal Data provided by Customer under the Agreement. In addition, Provider will not retain, use, or disclose any Personal Data provided by Customer under the Agreement except as necessary for providing the Service for Customer, as stated in the Agreement, or as permitted by Applicable Data Protection Laws. Provider certifies that it understands the restrictions of this paragraph and will comply with all Applicable Data Protection Laws. Provider will notify Customer if it can no longer meet its obligations under the CCPA.
Data Region	Customer selects a data residency region, United States or European Union, for its Mindsmith workspace. Provider stores Customer Personal Data at rest in the selected region and runs the Service's application, primary database, file storage, product analytics and the AI model endpoints used by the Service in that region, except for (a) the Approved Subprocessors identified on the Subprocessor list as Processing outside the region and (b) access by Provider personnel located in the United States for support, operations and security.

Common Paper Data Processing Agreement (Version 1.1) free to use under CC BY 4.0.

AI Features and Training	The Service uses large language models and other AI models hosted by the AI model Subprocessors on the Subprocessor list to generate and edit content, provide learner-facing AI agents and interactive conversations, and produce narration, translations, images and video. Provider will not use Customer Personal Data, or Customer's User Content as defined in the Agreement, to train or fine-tune AI models, and Provider's agreements with its AI model Subprocessors prohibit them from doing so. Customer Personal Data submitted to an AI model Subprocessor is used only to generate the requested output. Output is produced on Customer's instruction, and Customer is responsible for reviewing it before publishing it to learners.
Provider Service Data	Provider may Process information about the configuration, performance, security and use of the Service, including account, billing and support records of Customer's authorized users, as an independent Controller to provide, secure, support, bill for and improve the Service in accordance with Provider's Privacy Policy, and may create and use aggregated or de-identified data that does not identify Customer or any individual. This row does not permit any use excluded by the AI Features and Training row.
Excluded Data	Unless agreed with Provider in writing, Customer will not submit to the Service Special Category Data, payment card data, or government-issued identification numbers. Customer is responsible for giving learners any notice required for interactive features that record voice or free-text responses that Customer enables.
Children's Data	Customer may submit Personal Data of learners under 16 or the applicable age in Customer's jurisdiction to the Service, only to deliver Customer's learning programs. Customer is responsible for the lawful basis for this processing, including any parent, guardian, or school consent required by Applicable Data Protection Laws, and for giving learners and their parents age-appropriate privacy information, including that some features of the Service use AI. Provider will not use this data for advertising, or to profile learners for any purpose other than delivering Customer's learning programs. The rest of this DPA, including the AI Features and Training row, applies to it in full.
Liability for Restricted Transfer Terms	Notwithstanding Section 8.3 of the DPA Standard Terms, and to the maximum extent permitted by the EEA SCCs, the UK Addendum and Applicable Data Protection Laws, each party's liability to the other party arising out of a breach of the EEA SCCs or the UK Addendum is subject to the waivers, exclusions and limitations of liability stated in the Agreement. Nothing in this row limits either party's liability to an individual for that individual's data protection rights.
Deletion Timing	For Section 7.2 of the DPA Standard Terms, unless Customer instructs return first, Provider will delete Customer Personal Data from production systems within 60 days after the Agreement ends, and copies held in backups are overwritten in the normal backup rotation within a further 35 days. Personal Data retained in system logs for security and integrity purposes, or as required by Applicable Laws, remains subject to this DPA and is not used for any other purpose.

Restricted Transfers

Governing Member State	[x] EEA Transfers: Ireland [x] UK Transfers: Laws of England and Wales

Annex I(A) List of Parties

Data Exporter	Name: Customer Address: the address stated in the Agreement or on Customer's Mindsmith account Contact Person: the administrator contact on Customer's Mindsmith account, or the notice contact stated in the Agreement Activities relevant to transfer: See Annex 1(B) Role: Controller, or Processor where Customer Processes Customer Personal Data on behalf of its own Controllers (see Sections 1.2 and 3.2(b) of the DPA Standard Terms)

Data Importer	Name: Mindsmith Learning, Inc. Address: 3400 N. Ashton Blvd., Ste. 410, Lehi, UT 84043, United States Contact Person: Name: Zachary Allen Position: Co-Founder and CEO (privacy contact) Address: 3400 N. Ashton Blvd., Ste. 410, Lehi, UT 84043, United States; security@mindsmith.ai Activities relevant to transfer: See Annex 1(B) Role: Processor, or Subprocessor where Customer is a Processor EU representative (GDPR Article 27): Instant EU GDPR Representative Ltd, Office 2, 12A Lower Main Street, Lucan, Co. Dublin K78 X5P8, Ireland, contact@gdprlocal.com UK representative (UK GDPR Article 27): GDPRLocal Ltd., 1st Floor Front Suite, 27-29 North Street, Brighton BN1 1EB, United Kingdom, contact@gdprlocal.com

Annex I(B) Description of Transfer and Processing Activities

Service	Mindsmith, the AI-powered eLearning authoring and delivery platform described in the Agreement, including published courses, learner delivery, integrations and support.
Categories of Data Subjects	[x] Customer's employees, contractors and administrators who author, manage or review content [x] Learners who take courses published by Customer, who may be Customer's employees, contractors, customers, partners, students (including children, as described in the Children's Data row) or members of the public depending on how Customer publishes [x] Users provisioned through Customer's identity provider [x] Customer personnel who contact Provider support
Categories of Personal Data	[x] Name [x] Email address, for authors and administrators and, where Customer's deployment captures it, for learners [x] Phone number, only for learners Customer invites by SMS where Customer uses the SMS course invitation feature [x] Profile picture, where a user provides one or it is supplied by the user's sign-in provider [x] Workspace membership, role and permissions; for users provisioned from Customer's identity provider, the name and email address received from that provider [x] Authentication data such as password hashes and single sign-on identifiers [x] Billing contact email for the Customer account. Payment card details and billing addresses are collected and processed by Provider's payment processor, listed on the Subprocessor list, and are not stored by Provider [x] User activity and technical data such as IP address, browser and device information, usage telemetry, and session replay of authoring sessions with text inputs masked [x] Learning records such as course progress, scores, quiz and assessment responses, free-text answers, engagement and completion records, certificates, and learner identifiers supplied by Customer's learning management system [x] Interactive content data such as the text of conversations with AI agents, prompts submitted to AI features and, where Customer enables voice conversations, recorded audio and transcripts [x] Content data: Personal Data contained in documents, media and content that Customer uploads or generates, at Customer's discretion [x] Support communications with Provider
Special Category Data Is special category data Processed?	[ ] Yes [x] No Voice recordings made by interactive conversation features are not Processed to uniquely identify individuals. See the Excluded Data row.
Frequency of Transfer	[x] Continuous, for the term of the Agreement

Nature and Purpose of Processing	Provider will Process Customer Personal Data as instructed in Section 2.3 of the DPA Standard Terms. The nature of processing includes: [x] Receiving data, including collection, accessing, retrieval, recording, and data entry [x] Holding data, including storage, organization, and structuring [x] Using data, including analysis, consultation, testing, and AI inference to generate content and responses. The Service does not make automated decisions that produce legal or similarly significant effects on individuals [x] Updating data, including correcting, adaptation, alteration, alignment, and combination [x] Protecting data, including restricting, encrypting, and security testing [x] Sharing data, including disclosure, dissemination, allowing access, or otherwise making available, to Approved Subprocessors and to systems Customer connects [x] Returning data to the data exporter or data subject [x] Erasing data, including destruction and deletion The purpose of the Processing is to host, generate, edit, publish and deliver eLearning content; deliver courses to learners and record their progress, responses and completions; provide learner-facing AI agents and interactive conversations in text and, where Customer enables it, voice; produce narration, translations, images and video; authenticate users, including through single sign-on and directory synchronization; provide reporting and analytics to Customer; integrate with Customer's learning management system, collaboration tools and other systems Customer connects; provide support; and operate, secure, monitor and maintain the Service.
Duration of Processing	**Provider** will process Customer Personal Data as long as required (i) to conduct the Processing activities instructed in Section 2.2(a)-(d) of the Standard Terms; or (ii) by Applicable Laws.

Annex I(C)

Competent Supervisory Authority	The supervisory authority will be the supervisory authority of the data exporter, as determined in accordance with Clause 13 of the EEA SCCs or the relevant provision of the UK Addendum.

Annex II

Technical and Organizational Security Measures	[x] See Security Policy [x] Pseudonymization and encryption of personal data: Customer Personal Data is encrypted in transit using TLS 1.2 or higher and at rest using AES-256 or equivalent mechanisms provided by the underlying cloud platforms. Privileged access to encryption keys is restricted to authorized personnel with a documented business need. Sensitive data is scrubbed from error monitoring before transmission, and session replay masks text inputs. [x] Ensuring ongoing confidentiality, integrity, availability, and resilience of processing systems and services: Production systems run on enterprise cloud infrastructure with redundancy and high availability. The production network is segregated from non-production environments. Network and host-based firewalls and hardening standards are documented and reviewed at least annually. Authentication to production systems requires unique credentials or authorized cryptographic keys. [x] Ability to restore the availability of and access to Customer Personal Data in a timely manner following a physical or technical incident: Provider maintains documented business continuity and disaster recovery plans, tested at least annually. Backups of customer data are configured under Provider's data backup policy. Recovery time and recovery point objectives are maintained internally and available to Customer on request, subject to confidentiality. [x] Regular testing, assessment, and evaluation of the effectiveness of technical and organizational measures used to secure Processing:

Independent penetration testing at least annually, external vulnerability scans at least quarterly with critical and high findings tracked to remediation, annual control self-assessments, continuous control monitoring through a compliance management platform, and a SOC 2 Type II examination.

[x] User identification and authorization process and protection:
Role-based access with manager approval and least privilege. Multi-factor authentication for production systems and single sign-on for internal systems where supported. Access is reviewed periodically and revoked for departing personnel under Provider's termination procedures.

[x] Protecting Customer Personal Data during transmission (in transit):
TLS 1.2 or higher for all data transmitted over public networks, including transmission to Subprocessors.

[x] Protecting Customer Personal Data during storage (at rest):
AES-256 or equivalent encryption at rest across Provider's cloud infrastructure, backups and Subprocessor systems. Customer Personal Data is stored in the region Customer selects, United States or European Union, as described in the Data Region row.

[x] Physical security where Customer Personal Data is processed:
The Service runs entirely on third-party cloud infrastructure. Provider operates no data centers. Physical security is the responsibility of the cloud providers, each of which maintains ISO 27001 and SOC 2 attestations available from the provider.

[x] Events logging:
Centralized log management captures security-relevant events from production systems. An intrusion detection system monitors network activity, and monitoring tools alert on predefined thresholds. Logs are retained for periods consistent with Provider's data retention policy.

[x] Systems configuration, including default configuration:
Documented hardening standards, configuration management for consistent deployment, security testing in the continuous integration and deployment pipeline, and production deployment restricted to authorized personnel.

[x] Internal IT and IT security governance and management:
Documented information security policies reviewed at least annually, formally assigned security roles, management oversight with reporting to the board of directors, background checks at hire, signed confidentiality agreements, and security awareness training within thirty days of hire and annually.

[x] Certification or assurance of processes and products:
SOC 2 Type II examination (Security trust services criteria) by an independent CPA firm. Reports and penetration test summaries are available through the Trust Center under confidentiality.

[x] Ensuring data minimization:
Customer controls what content it uploads and which learner data collection and interactive features it enables. Provider Processes only the data needed to provide the Service.

[x] Ensuring data quality:
Customer and its authorized users can view and correct Customer Personal Data through the Service.

[x] Ensuring limited data retention:
Customer Personal Data is deleted at the end of the Agreement under Section 7 of the DPA Standard Terms. AI observability traces of prompts and responses are retained for 30 days. Backups are rotated under Provider's backup policy.

[x] Ensuring accountability:

Common Paper Data Processing Agreement (Version 1.1) free to use under CC BY 4.0.

Vendor management program with an inventory of critical Subprocessors, written Subprocessor agreements with confidentiality, privacy and transfer commitments, an incident response plan tested at least annually, a designated privacy contact, and appointed EU and UK representatives.

[x] Allowing data portability and ensuring erasure:
Customer can export course content and reporting data through the Service and delete Customer Personal Data through the Service during the term. Deletion at the end of the Agreement is described in Section 7 of the DPA Standard Terms.

Provider and Customer have not changed the DPA Standard Terms except for the details on the Cover Page above. By signing this Cover Page, each party agrees to enter into this DPA as of the last date of signature below.

	PROVIDER: Mindsmith Learning, Inc.	CUSTOMER: [Customer legal name]
Signature		
Print Name		
Title		
Date		

Common Paper Data Processing Agreement (Version 1.1) free to use under CC BY 4.0.

1. Processor and Subprocessor Relationships

1.1 Provider as Processor. In situations where **Customer** is a Controller of the Customer Personal Data, **Provider** will be deemed a Processor that is Processing Personal Data on behalf of **Customer**.

1.2 Provider as Subprocessor. In situations where **Customer** is a Processor of the Customer Personal Data, **Provider** will be deemed a Subprocessor of the Customer Personal Data.

2. Processing

2.1 Processing Details. Annex I(B) on the Cover Page describes the subject matter, nature, purpose, and duration of this Processing, as well as the **Categories of Personal Data** collected and **Categories of Data Subjects**.

2.2 Processing Instructions. **Customer** instructs **Provider** to Process Customer Personal Data: (a) to provide and maintain the Service; (b) as may be further specified through **Customer's** use of the Service; (c) as documented in the **Agreement**; and (d) as documented in any other written instructions given by **Customer** and acknowledged by **Provider** about Processing Customer Personal Data under this DPA. **Provider** will abide by these instructions unless prohibited from doing so by Applicable Laws. **Provider** will immediately inform **Customer** if it is unable to follow the Processing instructions. **Customer** has given and will only give instructions that comply with Applicable Laws.

2.3 Processing by Provider. **Provider** will only Process Customer Personal Data in accordance with this DPA, including the details in the Cover Page. If **Provider** updates the Service to update existing or include new products, features, or functionality, **Provider** may change the **Categories of Data Subjects**, **Categories of Personal Data**, **Special Category Data**, **Special Category Data Restrictions or Safeguards**, **Frequency of Transfer**, **Nature and Purpose of Processing**, and **Duration of Processing** as needed to reflect the updates by notifying **Customer** of the updates and changes.

2.4 Customer Processing. Where **Customer** is a Processor and **Provider** is a Subprocessor, **Customer** will comply with all Applicable Laws that apply to **Customer's** Processing of Customer Personal Data. **Customer's** agreement with its Controller will similarly require **Customer** to comply with all Applicable Laws that apply to **Customer** as a Processor. In addition, **Customer** will comply with the Subprocessor requirements in **Customer's** agreement with its Controller.

2.5 Consent to Processing. **Customer** has complied with and will continue to comply with all Applicable Data Protection Laws concerning its provision of Customer Personal Data to **Provider** and/or the Service, including making all disclosures, obtaining all consents, providing adequate choice, and implementing relevant safeguards required under Applicable Data Protection Laws.

2.6 Subprocessors.

(a) **Provider** will not provide, transfer, or hand over any Customer Personal Data to a Subprocessor unless **Customer** has approved the Subprocessor. The current list of **Approved Subprocessors** includes the identities of the Subprocessors, their country of location, and their anticipated Processing tasks. **Provider** will inform **Customer** at least 10 business days in advance and in writing of any intended changes to the **Approved Subprocessors** whether by addition or replacement of a Subprocessor, which allows **Customer** to have enough time to object to the changes before the **Provider** begins using the new Subprocessor(s). **Provider** will give **Customer** the information necessary to allow **Customer** to exercise its right to object to the change to **Approved Subprocessors**. **Customer** has 30 days after notice of a change to the **Approved Subprocessors** to object, otherwise **Customer** will be deemed to accept the changes. If **Customer** objects to the change within 30 days of notice, **Customer** and **Provider** will cooperate in good faith to resolve **Customer's** objection or concern.

(b) When engaging a Subprocessor, **Provider** will have a written agreement with the Subprocessor that ensures the Subprocessor only accesses and uses Customer Personal Data (i) to the extent required to perform the obligations subcontracted to it, and (ii) consistent with the terms of **Agreement**.

(c) If the GDPR applies to the Processing of Customer Personal Data, (i) the data protection obligations described in this DPA (as referred to in Article 28(3) of the GDPR, if applicable) are also imposed on the Subprocessor, and (ii) **Provider's** agreement with the Subprocessor will incorporate these obligations, including details about how **Provider** and its Subprocessor will coordinate to respond to inquiries or requests about the Processing of Customer Personal Data. In addition, **Provider** will share, at **Customer's** request, a copy of its agreements (including any amendments) with its Subprocessors. To the extent necessary to protect business secrets or other confidential information, including personal data, **Provider** may redact the text of its agreement with its Subprocessor prior to sharing a copy.

(d) **Provider** remains fully liable for all obligations subcontracted to its Subprocessors, including the acts and omissions of its Subprocessors in Processing Customer Personal Data. **Provider** will notify **Customer** of any failure by its Subprocessors to fulfill a material obligation about Customer Personal Data under the agreement between **Provider** and the Subprocessor.

3. Restricted Transfers

3.1 Authorization. **Customer** agrees that **Provider** may transfer Customer Personal Data outside the EEA, the United Kingdom, or other relevant geographic territory as necessary to provide the Service. If **Provider** transfers Customer Personal Data to a territory for which the European Commission or other relevant supervisory authority has not issued an adequacy decision, **Provider** will implement appropriate safeguards for the transfer of Customer Personal Data to that territory consistent with Applicable Data Protection Laws.

3.2 Ex-EEA Transfers. **Customer** and **Provider** agree that if the GDPR protects the transfer of Customer Personal Data, the transfer is from **Customer** from within the EEA to **Provider** outside of the EEA, and the transfer is not governed by an adequacy decision made by the European Commission, then by entering into this DPA, **Customer** and **Provider** are deemed to have signed the EEA SCCs and their Annexes, which are incorporated by reference. Any such transfer is made pursuant to the EEA SCCs, which are completed as follows:

(a) Module Two (Controller to Processor) of the EEA SCCs apply when **Customer** is a Controller and **Provider** is Processing Customer Personal Data for **Customer** as a Processor.

(b) Module Three (Processor to Sub-Processor) of the EEA SCCs apply when **Customer** is a Processor and **Provider** is Processing Customer Personal Data on behalf of **Customer** as a Subprocessor.

(c) For each module, the following applies (when applicable):

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

(ii) In Clause 9, Option 2 (general written authorization) applies, and the minimum time period for prior notice of Subprocessor changes is 10 business days;

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

(iv) All square brackets in Clause 13 are removed;

(v) In Clause 17 (Option 1), the EEA SCCs will be governed by the laws of **Governing Member State**;

(vi) In Clause 18(b), disputes will be resolved in the courts of the **Governing Member State**; and

(vii) The Cover Page to this DPA contains the information required in Annex I, Annex II, and Annex III of the EEA SCCs.

3.3 Ex-UK Transfers. **Customer** and **Provider** agree that if the UK GDPR protects the transfer of Customer Personal Data, the transfer is from **Customer** from within the United Kingdom to **Provider** outside of the United Kingdom, and the transfer is not governed by an adequacy decision made by the United Kingdom Secretary of State, then by entering into this DPA, **Customer** and **Provider** are deemed to have signed the UK Addendum and their Annexes, which are incorporated by reference. Any such transfer is made pursuant to the UK Addendum, which is completed as follows:

(a) Section 3.2 of this DPA contains the information required in Table 2 of the UK Addendum.

(b) Table 4 of the UK Addendum is modified as follows: Neither party may end the UK Addendum as set out in Section 19 of the UK Addendum; to the extent ICO issues a revised Approved Addendum under Section 18 of the UK Addendum, the parties will work in good faith to revise this DPA accordingly.

(c) The Cover Page contains the information required by Annex 1A, Annex 1B, Annex II, and Annex III of the UK Addendum.

3.4 Other International Transfers. For Personal Data transfers where Swiss law (and not the law in any EEA member state or the United Kingdom) applies to the international nature of the transfer, references to the GDPR in Clause 4 of the EEA SCCs are, to the extent legally required, amended to refer to the Swiss Federal Data Protection Act or its successor instead, and the concept of supervisory authority will include the Swiss Federal Data Protection and Information Commissioner.

4. Security Incident Response

Upon becoming aware of any Security Incident, **Provider** will: (a) notify **Customer** without undue delay when feasible, but no later than 72 hours after becoming aware of the Security Incident; (b) provide timely information about the Security Incident as it becomes known or as is reasonably requested by **Customer**; and (c) promptly take reasonable steps to contain and investigate the Security Incident. **Provider's** notification of or response to a Security Incident as required by this DPA will not be construed as an acknowledgment by **Provider** of any fault or liability for the Security Incident.

5. Audit & Reports

5.1 Audit Rights. **Provider** will give **Customer** all information reasonably necessary to demonstrate its compliance with this DPA and **Provider** will allow for and contribute to audits, including inspections by **Customer**, to assess **Provider's** compliance with this DPA. However, **Provider** may restrict access to data or information if **Customer's** access to the information would negatively impact **Provider's** intellectual property rights, confidentiality obligations, or other obligations under Applicable Laws. **Customer** acknowledges and agrees that it will only exercise its audit rights under this DPA and any audit rights granted by Applicable Data Protection Laws by instructing **Provider** to comply with the reporting and due diligence requirements below. **Provider** will maintain records of its compliance with this DPA for 3 years after the DPA ends.

5.2 Security Reports. **Customer** acknowledges that **Provider** is regularly audited against the standards defined in the **Security Policy** by independent third-party auditors. Upon written request, **Provider** will give **Customer**, on a confidential basis, a summary copy of its then-current Report so that **Customer** can verify **Provider's** compliance with the standards defined in the **Security Policy**.

5.3 Security Due Diligence. In addition to the Report, **Provider** will respond to reasonable requests for information made by **Customer** to confirm **Provider's** compliance with this DPA, including responses to information security, due diligence, and audit questionnaires, or by giving additional information about its information security program. All such requests must be in writing and made to the **Provider Security Contact** and may only be made once a year.

6. Coordination & Cooperation

6.1 Response to Inquiries. If **Provider** receives any inquiry or request from anyone else about the Processing of Customer Personal Data, **Provider** will notify **Customer** about the request and **Provider** will not respond to the request without **Customer's** prior consent. Examples of these kinds of inquiries and requests include a judicial or administrative or regulatory agency order about Customer Personal Data where notifying **Customer** is not prohibited by Applicable Law, or a request from a data subject. If allowed by Applicable Law, **Provider** will follow **Customer's** reasonable instructions about these requests, including providing status updates and other information reasonably requested by **Customer**. If a data subject makes a valid request under Applicable Data Protection Laws to delete or opt out of **Customer's** giving of Customer Personal Data to **Provider**, **Provider** will assist **Customer** in fulfilling the request according to the Applicable Data Protection Law. **Provider** will cooperate with and provide reasonable assistance to **Customer**, at **Customer's** expense, in any legal response or other procedural action taken by **Customer** in response to a third-party request about **Provider's** Processing of Customer Personal Data under this DPA.

6.2 DPIAs and DTIAs. If required by Applicable Data Protection Laws, **Provider** will reasonably assist **Customer** in conducting any mandated data protection impact assessments or data transfer impact assessments and consultations with relevant data protection authorities, taking into consideration the nature of the Processing and Customer Personal Data.

7. Deletion of Customer Personal Data

7.1 Deletion by Customer. **Provider** will enable **Customer** to delete Customer Personal Data in a manner consistent with the functionality of the Services. **Provider** will comply with this instruction as soon as reasonably practicable except where further storage of Customer Personal Data is required by Applicable Law.

7.2 Deletion at DPA Expiration.

(a) After the DPA expires, **Provider** will return or delete Customer Personal Data at **Customer's** instruction unless further storage of Customer Personal Data is required or authorized by Applicable Law. If return or destruction is impracticable or prohibited by Applicable Laws, **Provider** will make reasonable efforts to prevent additional Processing of Customer Personal Data and will continue to protect the Customer Personal Data remaining in its possession, custody, or control. For example, Applicable Laws may require **Provider** to continue hosting or Processing Customer Personal Data.

(b) If **Customer** and **Provider** have entered the EEA SCCs or the UK Addendum as part of this DPA, **Provider** will only give **Customer** the certification of deletion of Personal Data described in Clause 8.1(d) and Clause 8.5 of the EEA SCCs if **Customer** asks for one.

8. Limitation of Liability

8.1 Liability Caps and Damages Waiver. **To the maximum extent permitted under Applicable Data Protection Laws, each party's total cumulative liability to the other party arising out of or related to this DPA will be subject to the waivers, exclusions, and limitations of liability stated in the Agreement.**

8.2 Related-Party Claims. **Any claims made against Provider or its Affiliates arising out of or related to this DPA may only be brought by the Customer entity that is a party to the Agreement.**

8.3 Exceptions. This DPA does not limit any liability to an individual about the individual's data protection rights under Applicable Data Protection Laws. In addition, this DPA does not limit any liability between the parties for violations of the EEA SCCs or UK Addendum.

9. Conflicts Between Documents

This DPA forms part of and supplements the **Agreement**. If there is any inconsistency between this DPA, the **Agreement**, or any of their parts, the part listed earlier will control over the part listed later for that inconsistency: (1) the EEA SCCs or the UK Addendum, (2) this DPA, and then (3) the **Agreement**.

10. Term of Agreement

This DPA will start when **Provider** and **Customer** agree to a Cover Page for the DPA and sign or electronically accept the **Agreement** and will continue until the **Agreement** expires or is terminated. However, **Provider** and **Customer** will each remain subject to the obligations in this DPA and Applicable Data Protection Laws until **Customer** stops transferring Customer Personal Data to **Provider** and **Provider** stops Processing Customer Personal Data.

11. Definitions.

11.1 "**Applicable Laws**" means the laws, rules, regulations, court orders, and other binding requirements of a relevant government authority that apply to or govern a party.

11.2 "**Applicable Data Protection Laws**" means the Applicable Laws that govern how the Service may process or use an individual's personal information, personal data, personally identifiable information, or other similar term.

11.3 "**Controller**" will have the meaning(s) given in the Applicable Data Protection Laws for the company that determines the purpose and extent of Processing Personal Data.

11.4 "**Cover Page**" means a document that is signed or electronically accepted by the parties that incorporates these DPA Standard Terms and identifies **Provider**, **Customer**, and the subject matter and details of the data processing.

11.5 "**Customer Personal Data**" means Personal Data that **Customer** uploads or provides to **Provider** as part of the Service and that is governed by this DPA.

11.6 "**DPA**" means these DPA Standard Terms, the Cover Page between **Provider** and **Customer**, and the policies and documents referenced in or attached to the Cover Page.

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

11.8 "**European Economic Area**" or "**EEA**" means the member states of the European Union, Norway, Iceland, and Liechtenstein.

11.9 "**GDPR**" means European Union Regulation 2016/679 as implemented by local law in the relevant EEA member nation.

11.10 "**Personal Data**" will have the meaning(s) given in the Applicable Data Protection Laws for personal information, personal data, or other similar term.

11.11 "**Processing**" or "**Process**" will have the meaning(s) given in the Applicable Data Protection Laws for any use of, or performance of a computer operation on, Personal Data, including by automatic methods.

11.12 "**Processor**" will have the meaning(s) given in the Applicable Data Protection Laws for the company that Processes Personal Data on behalf of the Controller.

11.13 "**Report**" means audit reports prepared by another company according to the standards defined in the Security Policy on behalf of **Provider**.

11.14 "**Restricted Transfer**" means (a) where the GDPR applies, a transfer of personal data from the EEA to a country outside of the EEA which is not subject to an adequacy determination by the European Commission; and (b) where the UK GDPR applies, a transfer of personal

data from the United Kingdom to any other country which is not subject to adequacy regulations adopted pursuant to Section 17A of the United Kingdom Data Protection Act 2018.

11.15 "**Security Incident**" means a Personal Data Breach as defined in Article 4 of the GDPR.

11.16 "**Service**" means the product and/or services described in the **Agreement**.

11.17 "**Special Category Data**" will have the meaning given in Article 9 of the GDPR.

11.18 "**Subprocessor**" will have the meaning(s) given in the Applicable Data Protection Laws for a company that, with the approval and acceptance of Controller, assists the Processor in Processing Personal Data on behalf of the Controller.

11.19 "**UK GDPR**" means European Union Regulation 2016/679 as implemented by section 3 of the United Kingdom's European Union (Withdrawal) Act of 2018 in the United Kingdom.

11.20 "**UK Addendum**" means the international data transfer addendum to the EEA SCCs issued by the Information Commissioner for Parties making Restricted Transfers under S119A(1) Data Protection Act 2018.

Common Paper Data Processing Agreement (Version 1.1) free to use under CC BY 4.0.