Privacy and Data Security Addendum - September 2026

This Privacy and Data Security Addendum (the "**Addendum**") forms an integral part of the Terms of Use and any form, statement of work, or other written or electronic ordering document incorporating those Terms of Use by reference (collectively, the "**Agreement**"), entered into between Alma Labs Ltd. or the applicable affiliate identified in the Agreement (the "**Company**") and the customer identified in the Agreement (the "**Customer**") (each, a "**Party**" and together, the "**Parties**").

In accordance with the mutual commitments detailed below, the Parties hereby agree that the terms and conditions detailed below shall be attached as an addendum to the Agreement and shall constitute an integral part thereof.

1. **Definitions**

1.1. "**Customer's Personal Data**" means any Personal Data contained in Customer Data and Processed by the Company on behalf of the Customer in connection with the Services, as further described in **Appendix A**.

1.2. "**Process(ing)**", "**Controller**", "**Processor**" and "**Personal Data**" shall have the meanings given to them, or equivalent meanings, under the Privacy Laws.

1.3. "**Privacy Laws**" means applicable laws and regulations relating to the Processing of Personal Data, including, to the extent applicable to the relevant Processing, the **Privacy Protection Law**, 1981, the Privacy Protection Regulations (Data Security), 2017, and any other applicable data protection or privacy laws.

1.4. "**Services**" means the Solution and any related services to be provided by the Company in accordance with the Agreement.

2. **Company's Declarations and Commitments**

The Company declares and commits to the Customer as follows:

2.1. It shall be entitled to Process the Customer's Personal Data specified in **Appendix A** only, and solely for the purposes of the Agreement that are detailed in **Appendix A**.

2.2. It shall implement and maintain appropriate administrative, technical, physical and organizational security measures, taking into account the nature of Customer's Personal Data and the risks involved, in order to protect Customer's Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer's Personal Data.

2.3. Access to Customer's Personal Data shall be limited to authorized individuals acting on the Company's behalf and only as necessary for the performance of the Services or any other Processing expressly permitted under the Agreement and this Addendum.

2.4. It shall ensure that its authorized personnel are aware of the confidential nature of Customer's Personal Data, have received appropriate training regarding their responsibilities, are subject to confidentiality obligations, and do not use unlawful or unauthorized databases in the provision of the Services to the Customer.

2.5. It shall implement measures designed to maintain logical segregation of Customer's Personal Data from data of other customers and from data used by the Company for other

purposes, taking into account the nature of the Services and the Company's systems architecture.

3. **Data Security Incident**

3.1. In the event of a data security incident concerning the integrity of the Customer's Personal Data, unauthorized use thereof, or breach of permissions ("**Security Incident**"), the Company undertakes:

3.1.1. to notify the Customer about the Security Incident as soon as possible and in any case no later than 48 hours from the time it became aware of the Security Incident; and

3.1.2. to provide the Customer with all the information necessary for fulfilling its obligations under applicable Privacy Laws, including reporting obligations to the relevant authority.

3.2. The Company shall reasonably cooperate with the Customer in connection with a Security Incident affecting Customer's Personal Data.

3.3. The Company shall not be responsible to the extent that a Security Incident results from the Customer's instructions, systems, acts or omissions, or from the Customer's failure to take actions required under applicable law or the Agreement.

4. **Reporting and Audit**

4.1. At Customer's request, the Company shall provide the Customer with an annual written report detailing its compliance with the applicable Privacy Laws concerning the performance of the Services.

4.2. The Customer may, once per calendar year, conduct an audit of the Company's records, procedures, and facilities to ensure compliance with the requirements of this Appendix. Such an audit may be conducted by the Customer itself or a third-party auditor subject to a confidentiality obligation, and subject to coordinating the audit with the Company.

5. **Data Subjects Rights**

The Company shall promptly notify the Customer of any request received from a data subject or competent authority concerning Customer's Personal Data and shall provide reasonable assistance to the Customer as necessary for the Customer to comply with applicable Privacy Laws regarding such requests.

6. **Sub-processors**

6.1. The Customer hereby grants the Company a general authorization to engage third parties providing data Processing services (each, a "**Sub-processor**") to Process Customer's Personal Data, provided that such Sun-processors are materially subject to relevant commitments as set forth in this Addendum and provided that the Company remains responsible in accordance with this Addendum for the acts and omissions of its Sub-processors in connection with the Processing of Customer's Personal Data. The Company's then-current list of authorized Sub-processors, including the services performed and the territory in which Processing takes place, shall be made available upon request.

6.2. The Company may add or replace a Sub-processor from time to time by sending a notice to the Customer. If the Customer reasonably objects to a new or replacement Sub-processor on documented data protection grounds, Customer shall notify Company of such objection within 7 days from Company's notice and the Parties will discuss the objection in good faith.

7. **Deletion of Personal Data**

7.1. Upon termination or expiration of the Agreement, and subject to Section 7.2 below, the Company shall, at the Customer's written instruction, delete Customer's Personal Data Processed by the Company under this Addendum. If the Customer does not provide instructions within a reasonable period after termination or expiration, the Company may delete Customer's Personal Data in accordance with its standard retention practices.

7.2. The Company may retain Customer's Personal Data to the extent required by applicable law, for legal defense purposes, or in routine backup or archival systems until deletion occurs in the ordinary course, provided that the Company shall continue to protect such retained data in accordance with this Addendum for so long as it is retained.

8. **Limitation of Liability**

The liability of each Party arising out of or in connection with this Addendum shall be subject to the exclusions, limitations and aggregate cap on liability set out in the Agreement.

9. **Miscellaneous**

9.1. This Addendum shall become effective as of the Effective Date of the Agreement and shall remain in effect until the later of: (a) the termination or expiration of the Agreement; and (b) the cessation of all Processing of Customer's Personal Data by the Company on behalf of the Customer.

9.2. In the event of a conflict between this Addendum and the Agreement with respect to such Processing, this Addendum shall prevail to the extent of that conflict.

9.3. Any delay, waiver, extension, or postponement by the Customer in exercising its rights or demanding compliance with the terms of this Addendum, including consent to deviate from the terms of this Addendum, shall not be considered a waiver of other rights, a precedent, or consent to other cases.

9.4. Except as expressly set forth in this Addendum, the notice, governing law, jurisdiction, dispute resolution, amendment and interpretation provisions of the Agreement shall apply to this Addendum.

Exhibit A

1. The Personal Data that the Company may process: Customer's Personal Data may include:

   1.1 with respect to “Be” platform - students, their parents or guardians, and teachers, identifiers and contact details; account and role information; school, class and organizational affiliation data; educational, performance and progress data; and user-generated content, prompts, responses and communications with the Solution;

   1.2 with respect to “Become” platform - adult learners, job seekers, employees and other individuals participating in the workforce, and their instructors, mentors or supervisors, identifiers and contact details; account and role information; workplace and organizational affiliation data; professional, employment, skills, qualifications, performance and progress data; and user-generated content, prompts, responses and communications with the Solution.

   1.3 In both cases, Customer's Personal Data may also include support requests; usage, log, device and telemetry data; and any other Personal Data submitted by or on behalf of Customer and/or user in connection with the Services.

2. Permitted Purposes for Processing Personal Data: The Company may Process Customer's Personal Data, as permitted under the Agreement and as necessary to: (a) provide, host, operate, support, maintain, secure, troubleshoot and administer the Services; (b) generate Customer-facing outputs, reports, dashboards and insights requested by the Customer; (c) respond to support requests; and (d) develop, test, train, validate, improve and enhance the Services, the Solution and the Company's systems, features and functionality.

3. Allowed Processing operations: collection, receipt, access, hosting, storage, organization, structuring, retrieval, consultation, use, analysis, transmission to authorized Sub-processors, pseudonymization, aggregation, de-identification where applicable, creation and use of De-identified Data, backup, deletion and destruction, in each case solely as necessary for the purposes described above.