Data Processing Addendum

Last Modified: June 7, 2024

This Data Protection Addendum ("DPA") is an attachment to the Agreement and only applies when, in delivery of the Services under the Agreement, Provider is processing the Consumer Personal Data of Customer's End Users.

THIS AGREEMENT TAKES EFFECT WHEN CUSTOMER CLICKS THE "AUTHORIZE" BUTTON DURING LOGIN OR BY ACCESSING OR USING THE SERVICES UNDER THE AGREEMENT (THE "EFFECTIVE DATE"). BY CLICKING ON THE "AUTHORIZE" BUTTON DURING LOGIN OR BY ACCESSING OR USING THE SERVICES UNDER THE AGREEMENT, CUSTOMER (A) ACKNOWLEDGES THAT CUSTOMER HAS READ AND UNDERSTANDS THIS DPA; (B) REPRESENTS AND WARRANTS THAT CUSTOMER HAS THE RIGHT, POWER, AND AUTHORITY TO ENTER INTO THIS DPA AND, IF ENTERING INTO THIS DPA FOR AN ORGANIZATION, THAT CUSTOMER HAS THE LEGAL AUTHORITY TO BIND THAT ORGANIZATION; AND (C) ACCEPTS THIS DPA AND AGREES THAT CUSTOMER IS LEGALLY BOUND BY ITS TERMS.

Article 1 - Definitions

Capitalized terms that are not defined in this DPA have the meaning given to them in Agreement between the parties.

1. **Addendum:** "Addendum" means this Data Processing Addendum, attached to the Agreement.

2. **Agreement**: "Agreement" means the Terms of Service published on Provider's site and any applicable order form(s) and statement of work(s) between the parties.

3. **Consumer Generated Content:** "Consumer Generated Content" means any data, file attachments, text, images, reports, personal information, or other content or material that is uploaded or submitted to the Services by End Users and is processed by Provider on behalf of Customer. For the avoidance of doubt, Consumer Generated Content does not include usage, statistical, or technical information that does not reveal the actual contents of the Consumer Generated Content.

4. **Consumer Personal Data:** "Consumer Personal Data" means any information Provider processes for Customer that (a) identifies or relates to an individual who can be identified directly or indirectly from that data alone or in combination with other information in Provider's possession, control, or that Provider is likely to have access to, and (b) the relevant Privacy and Data Protection Requirements otherwise define as personally identifiable information. Consumer Personal Data does not include DII.

5. **Customer:** "Customer" means you, your organization, your authorized employees, contractors or agents using our Site and Services.

6. **Data Subject:** "Data Subject" means an individual who is the subject of the Consumer

Personal Data and to whom or about whom the Consumer Personal Data relates or identifies, directly or indirectly.

7. **De-Identifiable Information (DII): "**De-Identifiable Information" means any information in any format or media from which all PII has been removed or obscured in a way that eliminates the risk of disclosure of the identity of the individual.

8. **End Users:** "End Users" means, depending on the type of Service provided by Provider, Customer's consumers or customers, Customer's employees, or other groups.

9. **NIST 800-63-3**: "NIST 800-63-3" means the National Institute of Standards and Technology ("NIST") Special Publication 800-63-3 Digital Identity Guidelines or, if finalized, the most recent revision to those guidelines.

10. **Personally Identifiable Information (PII):** "Personally Identifiable Information" or "PII" means Consumer Personal Data and Consumer Generated Content obtained by reason of the use of Provider's software, website, service, or app, including mobile apps, whether gathered by Provider or provided by Customer or its End Users. PII includes indirect identifiers, which is any information that, either alone or in aggregate, would allow a reasonable person to be able to identify a consumer to a reasonable certainty.

11. **Privacy and Data Protection Requirements:** "Privacy and Data Protection Requirements" means all applicable U.S. federal and state laws and regulations, including California Consumer Privacy Act of 2018 ("CCPA") as amended by the California Privacy Rights Act ("CPRA") relating to the processing, protection, or privacy of Consumer Personal Data.

12. **Processing, processes or process:** "Processing, processes, or process" means any activity that involves the use of Consumer Personal Data or that the relevant Privacy and Data Protection Requirements may otherwise include in the definition of processing, processes, or process. It includes obtaining, recording, or holding the data, or carrying out any operation or set of operations on the data including, but not limited to, organizing, amending, retrieving, using, disclosing, erasing, or destroying it. Processing also includes transferring Consumer Personal Information to third parties.

13. **Provider:** "Provider" means Stride Learning Intelligence Inc.

14. **Security Breach:** "Security Breach" means an unauthorized access, disclosure, or acquisition of Consumer Personal Data that compromises the security, confidentiality, or integrity of such data.

15. **Services:** "Services" means the services described in the Agreement.

16. **Subprocessor:** "Subprocessor" means a party (subcontractor or independent contractor) other

than Customer or Provider who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its software, and who has access to Consumer Personal Data.

Article 2 – Scope

1. **Consumer Personal Data to Be Provided**. In order to perform the Services described in the Agreement, Customer may provide to the Provider, or the Provider may process from Customer's End Users Consumer Personal Data.

2. **Agreement Termination**. This Addendum shall survive the termination of the Agreement and shall apply for as long as Provider maintains any Consumer Personal Data.

Article 3 – Data Ownership, Authorized Access

1. **Consumer Personal Data Property of Customer**. As between Customer and Provider, all Consumer Personal Data transmitted to the Provider by any person or entity pursuant to the Agreement is and will continue to be the property of and under the control of Customer. The Provider agrees that all copies of such Consumer Personal Data transmitted to the Provider are subject to this Addendum in the same manner as the original Consumer Personal Data. The parties agree that as between them, all rights, including all intellectual property rights in and to Consumer Personal Data contemplated per the Agreement, shall remain the exclusive property of Customer.

2. **Third Party Request**. Provider will maintain the confidentiality of all Consumer Personal Data, will not sell it to third parties, and will not disclose it to third parties unless this Addendum specifically authorizes the disclosure, or as required by law. This restriction does not apply to DII. Should a third party, including law enforcement and government entities, contact Provider with a request for Consumer Personal Data held by the Provider pursuant to the Agreement, the Provider shall promptly notify Customer in advance of a compelled disclosure to a third party unless legally prohibited.

3. **No Unauthorized Use**. Provider shall not process Consumer Personal Data for any purpose other than as explicitly specified in the Agreement or as allowed under this Addendum. Provider will not process Consumer Personal Data in a way that does not comply with this Addendum or with the Privacy and Data Protection Requirements.

4. **Subprocessors**. Provider shall enter into written agreements with all Subprocessors performing functions pursuant to or in fulfillment of the Agreement, whereby the Subprocessors agree to protect Consumer Personal Data in a manner consistent with the terms of this Addendum.

Article 4 – Duties of Customer

1. **Provide Data in Compliance With Privacy and Data Protection Requirements**. Customer shall provide Consumer Personal Data for the purposes of the Agreement to Provider in compliance with applicable Privacy and Data Protection Requirements.

2. **Reasonable Precautions**. Customer shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the Services.

3. **Unauthorized Access Notification**. Customer shall notify Provider promptly of any known or suspected unauthorized access to the Services. Customer will reasonably assist Provider's efforts to investigate and respond to any unauthorized access.

Article 5 – Duties of Provider

1. **Privacy Compliance**. Provider shall comply with all applicable Privacy and Data Protection Requirements, including but not limited to any and all requirements of a "service provider" or "processor" of Consumer Personal Data. Provider will reasonably assist Customer with meeting Customer's compliance obligations under the Privacy and Data Protection Requirements, considering the nature of Provider's processing and the information available to Provider.

2. **Authorized Use**. The data, including Consumer Personal Data, shared pursuant to the Agreement, including persistent unique identifiers, shall be used for no purpose other than providing the Services to Customer and its End Users as stated in the Agreement and/or otherwise authorized under the statutes referred to in subsection (1) of this Article 5.

3. **Employee Obligation**. Provider will limit Consumer Personal Data access to those of its employees who require Personal Information access to meet Provider's obligations under this Addendum and the Agreement, and the part or parts of the Consumer Personal Data that those employees strictly require for the performance of their duties. Provider shall require all employees who have access to Consumer Personal Data to comply with all applicable provisions of this Addendum with respect to the data shared under the Agreement, and will provide its employees with periodic training on the Privacy and Data Protection Requirements relating to handling Personal Information and how it applies to their particular duties.

4. **Rights of Data Subjects**. Without undue delay and in compliance with applicable Privacy and Data Protection Requirements, Provider shall, if necessary, with the assistance of Customer, address and timely respond to requests or complaints from Data Subjects related to Provider's processing of Consumer Personal Data under the Agreement and this Addendum and the exercise of such Data Subject's rights under the applicable Privacy and Data Protection Requirements. Provider shall take appropriate measures to facilitate such Data Subject requests and the exercise of Data Subject rights. Any information provided to the Data Subject shall be in an intelligible and easily accessible form, using clear and plain language.

5. **Disposition of Data**. Provider shall dispose or delete all Consumer Personal Data obtained under the Agreement when it is no longer needed for the purpose for which it was obtained, and transfer said data to Customer within sixty (60) days of the date of expiration or the earlier termination of the Agreement, provided Customer provides Provider with a written request to dispose or delete of such Consumer Personal Data. The duty to dispose of Consumer Personal Data shall not extend to data that has been de-identified in accordance with applicable Privacy and Data Protection Requirements. Upon receipt of a request from Customer, the Provider will promptly provide Customer with any specified portion of the Consumer Personal Data.

Article 6– Data Provisions

1. **Data Security**. The Provider agrees to abide by and maintain appropriate technical and organizational measures, consistent with industry standards as set forth by applicable Privacy and Data Protection Requirements, using commercially available technology to protect Consumer Personal Data from unauthorized processing, modification, copying, reproduction, display, storage, access, distribution, transfer, disclosure or acquisition by an unauthorized person.

2. **Data Breach**. In the event that Consumer Personal Data is accessed or obtained by an unauthorized individual, Provider shall provide prompt notification to Customer of the incident in accordance with applicable state and in federal law with respect to a data breach related to the Consumer Personal Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.

3. **Security Audit.** Provider agrees, at Customer's written request, and no more frequently than once a year, to promptly provide Customer with documentation regarding its safeguards for Consumer Personal Data. Provider shall also promptly provide Customer with a written plan to remediate any high severity identified security and privacy vulnerabilities in a timely manner, but in no event more than three months after they have been identified.