DATA PROCESSING AGREEMENT

This Data Processing Agreement ("DPA" or "Agreement"), entered into by the CPI customer identified on the applicable CPI services agreement for CPI services ("Customer") and the CPI company identified on such document ("CPI"), governs the processing of personal data that Customer uploads or otherwise provides CPI in connection with the services and the processing of any personal data that CPI uploads or otherwise provides to Customer in connection with the services.

This DPA is incorporated into the relevant CPI services agreement attached to or incorporated by reference previously executed by Customer, referred to generically in this DPA as the "CPI Contract". Collectively, the DPA (including the SCCs, as defined herein), the CPI Contract, and any applicable ordering documents are referred to in this DPA as the "Agreement". In the event of any conflict or inconsistency between any of the terms of the Agreement, the provisions of the following documents (in order of precedence) shall prevail: (a) the SCCs; (b) this DPA; (c) the CPI Contract; and (d) the applicable ordering document, if any, to the CPI Contract. Except as specifically amended in this DPA, the CPI Contract and any applicable ordering document remain unchanged and in full force and effect.

1. DEFINITIONS

"Controller-to-Controller SCCs" means the Standard Contractual Clauses (Controller to Controller Transfers - Set II) in the Annex to the European Commission Decision of December 27, 2004, as may be amended or replaced from time to time by the European Commission.

"Controller-to-Processor SCCs" means the Standard Contractual Clauses (Processors) in the Annex to the European Commission Decision of February 5, 2010, as may be amended or replaced from time to time by the European Commission.

"Customer Personal Data" means Personal Data (i) that Customer uploads or otherwise provides CPI in connection with its use of CPI's services or (ii) for which Customer is otherwise a data controller.

"Data Controller" means Customer.

"Data Processor" means CPI.

"Data Protection Requirements" means the Directive, the General Data Protection Regulation, Local Data Protection Laws, any subordinate legislation and regulation implementing the General Data Protection Regulation, and all Privacy Laws.

"Directive" means the EU Data Protection Directive 95/46/EC (as amended).

"EU Personal Data" means Personal Data the sharing of which pursuant to this Agreement is regulated by the Directive, the General Data Protection Regulation and Local Data Protection Laws.

"General Data Protection Regulation" means the European Union Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

"Local Data Protection Laws" means any subordinate legislation and regulation implementing the Directive or the General Data Protection Regulation which may apply to the Agreement.

"Personal Data" means information about an individual that (a) can be used to identify, contact or locate a specific individual, including data that Customer chooses to provide to CPI from services; (b) can be combined with other information that can be used to identify, contact or locate a specific individual; or (c) is defined as "personal data" or "personal information" by applicable laws or regulations relating to the collection, use, storage or disclosure of information about an identifiable individual.

"Personal Data Breach" means any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data.

"Privacy Laws" means all applicable laws, regulations, and other legal requirements relating to (a) privacy, data security, consumer protection, marketing, promotion, and text messaging, email, and other communications; and (b) the use, collection, retention, storage, security, disclosure, transfer, disposal, and other processing of any Personal Data.

"Process" and its cognates mean any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"SCCs" means all Controller-to-Processor SCCs and Controller-to-Controller SCCs entered into between the parties under the Agreement.

"Subprocessor" means any entity which provides processing services to CPI in furtherance of CPI's processing on behalf of Customer.

"Supervisory Authority" means an independent public authority which is established by a European Union member state pursuant to Article 51 of the General Data Protection Regulation.

2. NATURE OF DATA PROCESSING

Each party agrees to process Personal Data received under the Agreement only for the purposes set forth in the Agreement. For the avoidance of doubt, the categories of Personal Data processed and the categories of data subjects subject to this DPA are described in Schedule A to this DPA.

3. COMPLIANCE WITH LAWS

The parties shall each comply with their respective obligations under all applicable Data Protection Requirements.

4. CUSTOMER OBLIGATIONS

Customer agrees to:

4.1   Provide instructions to CPI and determine the purposes and general means of CPI's processing of Customer Personal Data in accordance with the Agreement; and

4.2   Comply with its protection, security and other obligations with respect to Customer Personal Data prescribed by Data Protection Requirements for data controllers by: (a) establishing and maintaining a procedure for the exercise of the rights of the individuals whose Customer Personal Data are processed on behalf of Customer; (b) processing only data that has been lawfully and validly collected and ensuring that such data will be relevant and proportionate to the respective uses; and (c) ensuring compliance with the provisions of this Agreement by its personnel or by any third-party accessing or using Customer Personal Data on its behalf.

5. CPI OBLIGATIONS

5.1   Processing Requirements. CPI will:

a.   Process Customer Personal Data (i) only for the purpose of providing, supporting and improving CPI's services (including to provide insights and other reporting), using appropriate technical and organizational security measures; and (ii) in compliance with the instructions received from Customer. CPI will not use or process the Customer Personal Data for any other purpose. CPI will promptly inform Customer in writing if it cannot comply with the requirements under Sections 5-8 of this DPA, in which case Customer may terminate the Agreement or take any other reasonable action, including suspending data processing operations;

b.   Inform Customer promptly if, in CPI's opinion, an instruction from Customer violates applicable Data Protection Requirements;

c.   If CPI is collecting Customer Personal Data from individuals on behalf of Customer, follow Customer's instructions regarding such Customer Personal Data collection (including with regard to the provision of notice and exercise of choice);

d.   Take commercially reasonable steps to ensure that (i) persons employed by it and (ii) other persons engaged to perform on CPI's behalf comply with the terms of the Agreement;

e.   Ensure that its employees, authorized agents and any Subprocessors are required to comply with and acknowledge and respect the confidentiality of the Customer Personal Data, including after the end of their respective employment, contract or assignment;

f.   If it intends to engage Subprocessors to help it satisfy its obligations in accordance with this DPA or to delegate all or part of the processing activities to such Subprocessors, (i) exclusive of the list of Subprocessors CPI employs at commencement of the CPI Contract, obtain the prior written consent of Customer to such subcontracting, such consent to not be unreasonably withheld; (ii) remain liable to Customer for the Subprocessors' acts and omissions with regard to data protection where such Subprocessors act on CPI's instructions; and (iii) enter into contractual arrangements with such Subprocessors binding them to provide the same level of data protection and information security to that provided for herein;

g.   Upon request, provide Customer with a summary of CPI's privacy and security policies; and

h.   Inform Customer if CPI undertakes an independent security review.

5.2   Notice to Customer. CPI will inform Customer if CPI becomes aware of:

a.   Any non-compliance by CPI or its employees with Sections 5-8 of this DPA or the Data Protection Requirements relating to the protection of Customer Personal Data processed under this DPA;

b.   Any legally binding request for disclosure of Customer Personal Data by a law enforcement authority, unless CPI is otherwise forbidden by law to inform Customer, for example to preserve the confidentiality of an investigation by law enforcement authorities;

c.   Any notice, inquiry or investigation by a Supervisory Authority with respect to Customer Personal Data; or

d.   Any complaint or request (in particular, requests for access to, rectification or blocking of Customer Personal Data) received directly from data subjects of Customer. CPI will not respond to any such request without Customer's prior written authorization.

5.3   Assistance to Customer. CPI will provide reasonable assistance to Customer regarding:

a.   Any requests from Customer data subjects in respect of access to or the rectification, erasure, restriction, portability, blocking or deletion of Customer Personal Data that CPI processes for Customer. In the event that a data subject sends such a request directly to CPI, CPI will promptly send such request to Customer;

b.   The investigation of Personal Data Breaches and the notification to the Supervisory Authority and Customer's data subjects regarding such Personal Data Breaches; and

c.   Where appropriate, the preparation of data protection impact assessments and, where necessary, carrying out consultations with any Supervisory Authority.

5.4   Required Processing. If CPI is required by Data Protection Requirements to process any Customer Personal Data for a reason other than providing the services described in the Agreement, CPI will inform Customer of this requirement in advance of any processing, unless CPI is legally prohibited from informing Customer of such processing (e.g., as a result of secrecy requirements that may exist under applicable EU member state laws).

5.5   Security. CPI will:

a.   Maintain appropriate organizational and technical security measures (including with respect to personnel, facilities, hardware and software, storage and networks, access controls, monitoring and logging, vulnerability and breach detection, incident response, and protection against unauthorized or accidental access, loss, alteration, disclosure or destruction of Customer Personal Data);

b.   Be responsible for the sufficiency of the security, privacy, and confidentiality safeguards of all CPI personnel with respect to Customer Personal Data and liable for any failure by such CPI personnel to meet the terms of this DPA;

c.   Take reasonable steps to confirm that all CPI personnel are protecting the security, privacy and confidentiality of Customer Personal Data consistent with the requirements of this DPA; and

d.   Notify Customer of any Personal Data Breach by CPI, its Subprocessors, or any other third-parties acting on CPI's behalf without undue delay and in any event within 48 hours of becoming aware of a Personal Data Breach.

6. AUDIT, CERTIFICATION

6.1   Supervisory Authority Audit. If a Supervisory Authority requires an audit of the data processing facilities from which CPI processes Customer Personal Data in order to ascertain or monitor Customer's compliance with Data Protection Requirements, CPI will cooperate with such audit. Customer is responsible for all costs and fees related to such audit, including all reasonable costs and fees for any and all time CPI expends for any such audit, in addition to the rates for services performed by CPI.

6.2   Audits. CPI must, upon Customer's written request (not to exceed one request per calendar year), certify compliance with Sections 5-8 of this DPA in writing. CPI will provide to Customer each year an opinion or

Service Organization Control report provided by an accredited, third-party audit firm under the Statement on Standards for Attestation Engagements (SSAE) No. 16 ("SSAE 16") (Reporting on Controls at a Service Organization) or the International Standard on Assurance Engagements (ISAE) 3402 ("ISAE 3402") (Assurance Reports on Controls at a Service Organization) standards applicable to the services under the Agreement (each such report, a "Report"). If a Report does not provide, in Customer's reasonable judgment, sufficient information to confirm CPI's compliance with the terms of this DPA, then Customer or an accredited third-party audit firm agreed to by both Customer and CPI may audit CPI's compliance with the terms of this DPA during regular business hours, with reasonable advance notice to CPI and subject to reasonable confidentiality procedures. Customer is responsible for all costs and fees related to such audit, including all reasonable costs and fees for any and all time CPI expends for any such audit, in addition to the rates for services performed by CPI. Before the commencement of any such audit, Customer and CPI shall mutually agree upon the scope, timing, and duration of the audit. Customer shall promptly notify CPI with information regarding any non-compliance discovered during the course of an audit. Customer may not audit CPI more than once annually.

7. DATA TRANSFERS

For transfers of EU Personal Data to CPI for processing by CPI in a jurisdiction other than a jurisdiction in the EU, the EEA, or the European Commission-approved countries providing 'adequate' data protection, CPI agrees it will (a) provide at least the same level of privacy protection for EU Personal Data as required under the U.S.-EU and U.S.-Swiss Privacy Shield frameworks; or (b) use the applicable form of the Controller-to-Processor SCCs. If data transfers under Section 7 of this DPA rely on Controller-to-Processor SCCs to enable the lawful transfer of EU Personal Data, as set forth in the preceding sentence, the parties agree that data subjects for whom a CPI entity processes EU Personal Data are third-party beneficiaries under the Controller-to-Processor SCCs. If CPI is unable or becomes unable to comply with these requirements, then EU Personal Data will be processed and used exclusively within the territory of a member state of the European Union and any movement of EU Personal Data to a non-EU country requires the prior written consent of Customer. CPI shall promptly notify Customer of any inability by CPI to comply with the provisions of this Section 7.

8. DATA RETURN AND DELETION

The parties agree that on the termination of the data processing services or upon Customer's reasonable request, CPI shall, and shall cause any Subprocessors to, at the choice of Customer, return all the Customer Personal Data and copies of such data to Customer or securely destroy them and demonstrate to the satisfaction of Customer that it has taken such measures, unless Data Protection Requirements prevent CPI from returning or destroying all or part of the Customer Personal Data disclosed. In such case, CPI agrees to preserve the confidentiality of the Customer Personal Data retained by it and that it will only actively process such Customer Personal Data after such date in order to comply with applicable laws.

9. CONTROLLER-TO-CONTROLLER SCENARIOS

Each party will, to the extent that it, along with the other party, acts as data controller, as the term is defined in applicable Data Protection Requirements, with respect to Personal Data, reasonably cooperate with the other party to enable the exercise of data protection rights as set forth in the General Data Protection Regulation and in other Data Protection Requirements. Where both parties each act as data controller with respect to Personal Data, and the transfer of data between the parties results in a transfer of EU Personal Data to a jurisdiction other than a jurisdiction in the EU, the EEA, or the European Commission-approved countries providing 'adequate' data protection, each party agrees it will (a) provide at least the same level of privacy protection for EU Personal Data as required under the U.S.-EU and U.S.-Swiss Privacy Shield frameworks; or (b) use the Controller-to-Controller SCCs, which are incorporated herein by reference. If data transfers under this DPA rely on Controller-to-Controller SCCs to enable the lawful transfer of Personal Data, as set forth in the preceding sentence, the parties agree that the following terms apply: (i) Data subjects for whom a Customer processes EU Personal Data are third-party beneficiaries under the Controller-to-Controller SCCs; (ii) Schedule A to this DPA shall apply as Annex B of the Controller-to-Controller SCCs; and (iii) for purpose of Section II(h), the data importer will process the EU Personal Data, at its option, in accordance with "the relevant provisions of any Commission decision pursuant to Article 25(6) of Directive 95/46/EC, where the data importer complies with the relevant provisions of such an authorization or decision and is based in a country to which such an authorization or decision pertains, but is not covered by such authorization or decision for the purposes of the transfer(s) of the personal data." The parties acknowledge and agree that each is acting independently as Data Controller with respect of Personal Information and the parties are not joint controllers as defined in the General Data Protection Regulation.

10. THIRD PARTY DATA PROCESSORS

Customer acknowledges that in the provision of some services, CPI, on receipt of instructions from Customer, may transfer Customer Personal Data to and otherwise interact with third party data processors. Customer agrees that if and to the extent such transfers occur, Customer is responsible for entering into separate contractual arrangements with such third party data processors binding them to comply with obligations in accordance with Data Protection Requirements. For avoidance of doubt, such third party data processors are not Subprocessors.

11. TERM

This DPA shall remain in effect as long as CPI carries out Personal Data processing operations on behalf of Customer or until the termination of the CPI Contract (and all Personal Data has been returned or deleted in accordance with Section 8 above).

12. GOVERNING LAW, JURISDICTION, AND VENUE

Notwithstanding anything in the Agreement to the contrary, this DPA shall be governed by the laws of the State of Maryland, U.S.A., and any action or proceeding related to this DPA (including those arising from non-

contractual disputes or claims) will be brought in the State of Maryland or such other jurisdiction as is required by law

SCHEDULE A

ANNEX B - DESCRIPTION OF THE TRANSFER

1. **Data Subjects.** The personal data transferred concern the following categories of data subjects:

Depending on the services used by the data exporter:

- Individual users of the Customer's services;
- Third parties that have, or may have, a commercial relationship with the data exporter (e.g. advertisers, customers, corporate subscribers and contractors).

2. **Purposes of the Transfer.** The transfer is made for the following purposes:

The transfer is intended to enable the data exporter to determine the purposes and means of the processing of personal data obtained through data importer's products to support the educational, sales or other business practices of the data exporter.

3. **Categories of Data.** The personal data transferred concern the following categories of data:

The data transferred is the personal data provided by the data exporter to the data importer in connection with its use of Customer's online learning or other services, referred to as Customer Personal Data in the CPI Contract. Such personal data may include first name, last name, email address and IP address.

4. **Recipients.** The personal data transferred may be disclosed only to the following recipients or categories of recipients:

Employees and other representatives of the data importer who have a legitimate business purpose for the processing of such personal data.

5. **Sensitive Data (if appropriate).** The personal data transferred concern the following categories of sensitive data:

None.

6. **Data Protection Registration Information of Data Exporter (where applicable)**.

None.

7. **Additional Useful Information (storage limits and other relevant information)**.

The personal data transferred between the parties may only be retained for the period of time permitted under the Agreement. The parties agree that each party will, to the extent that it, along with the other party, acts as a data controller with respect to Personal Data, reasonably cooperate with the other party to enable the exercise of data protection rights as set forth in the Data Protection Requirements.

8. **Contact Information.** Contact points for data protection enquiries:

Data importer: Signatory to the Agreement between the parties

Data exporter: Signatory to the Agreement between the parties