Class Technologies, Inc. Data Protection Addendum
Effective Date: 28 August 2023

This Data Protection Addendum (the "**Addendum**") is between Class Technologies, Inc. a Delaware corporation (referred to herein as "**Class**" or "**Service Provider**") and the Class Customer identified on the Order Form for the purchase of certain Class Services between the parties hereto (the "**Agreement**"), to which this Addendum is incorporated (referred to herein as the "**Data Controller**" or "**Customer**") and is effective as of the Order Form date (the "**DPA**"). The terms of this DPA are hereby incorporated by reference into the terms of the Agreement.

This DPA shall apply and govern the processing of Personal Data solely to the extent that: 1) Class is a data processor or service provider under the terms of applicable data protection law; 2) Data Controller is subject to the applicable data protection law; and 3) Class performs processing of Personal Data under the Agreement. The parties agree that for the purposes of this DPA, Customer is a Data Controller or Business and Class is a Data Processor or Service Provider.

1. **Definitions.** The following terms in this DPA shall have the following meanings:
    1. "**Applicable Law(s)**" means all applicable laws, regulations, and other legally binding requirements in any jurisdiction relating to privacy, data protection, data security, breach notification, or the Processing of Personal Data, including without limitation, to the extent applicable, the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq. and any associated regulations and amendments, ("**CCPA**"); the General Data Protection Regulation, Regulation (EU) 2016/679 ("**GDPR**"); the Swiss Federal Act on Data Protection ("**FADP**"); the United Kingdom Data Protection Act of 2018 ("**UK GDPR**").
    2. "**Contracted Business Purposes**" means the services described in Service Agreement for which Class may receive or access personal information as defined in the CCPA and subject to the CCPA, or as otherwise instructed by Customer.
    3. "**Data Controller**" refers to the natural or legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data, and for purposes of this DPA is identified above as the Data Controller;
    4. "**Data Processor**" refers to the natural or legal person which, alone or jointly with others, processes personal data on behalf of the data controller, and for the purposes of this DPA is Class; "**Data Subject**" shall have the meaning given to it in the applicable data protection laws;
    5. "**EU SCCs**" means the standard contractual clauses issued pursuant to the EU Commission Implementing Decision (EU) 2021/914 of 4 June 2021 for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, available at http://data.europa.eu/eli/dec_impl/2021/914/oj and completed as described in the "Data Transfers" section below.
    6. "**Technical and organizational security measures**" means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.
    7. "**Personal Data**" includes "personal data," "personal information," and "personally identifiable information," and such terms have the same meaning as defined by Applicable Law.
    8. "**Personal Data Breach**" means the accidental or unlawful destruction, loss, alteration, unauthorized disclosure or exfiltration of, or access to, EU Data Subject Personal Data.
    9. "**Process**" and "**Processing**" means any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, creating, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
    10. "**Security Breach"** means any accidental or unlawful acquisition, destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data.
    11. "**Sub-processor**" means any data processor affiliate or subcontractor engaged by Class for the processing of Personal Data.
    12. "**UK SCCs**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (available as of the Effective Date at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf), and completed as described in the "Data Transfers" section below.
2. **Nature and Purpose of the Processing.** The scope, nature, purposes, and duration of the processing, the types of Personal Data Processed, and the Data Subjects concerned are set forth in this DPA, including its Schedules. The details provided in

Schedule A are deemed to satisfy any requirement to provide some or all of such details under any Applicable Law. The processing is being conducted solely for the purpose set forth in the Agreement for the applicable Class services detailed in the Agreement (the "Services") and for the term of the Agreement, which may include fulfilling requests for transcripts and other credential-types and admissions-related documents, including the processing of orders to have a specific document or record sent from a record holder to a record recipient. Class has no obligation to monitor the compliance of Customer's use of the Services with Applicable Law. The terms and conditions of the Agreement, including this DPA, along with Customer's configuration of any settings or options in the Services constitute Customer's complete and final instructions to Class regarding the processing of Personal Data, including for purposes of the UK SCCs and EU SCCs. Without limiting the foregoing:

1. Class will not process the Personal Data in a manner inconsistent with Class's role as Customer's "Service Provider" as such term is defined in the CCPA.
2. Class will not "sell" the Personal Data, as such term is defined in Applicable Laws.
3. Class will not "share" the Personal Data for purposes of "cross-context behavioral advertising" as defined in the CCPA or "targeted advertising," as such terms are defined in Applicable Laws.
4. Class will not otherwise Process the Personal Data for any purpose other than for the specific purposes set forth herein or outside of the direct business relationship with Customer.
5. Class will not attempt to re-identify any pseudonymized, anonymized, aggregate, or de-identified Personal Data without Customer's express written permission.
6. Class will comply with any applicable restrictions under Applicable Laws on combining Personal Data with personal data that Class receives from, or on behalf of, another person or persons, or that Class collects from any interaction between it and a data subject.
7. Class will provide the same level of protection for Personal Data as is required under the CCPA applicable to Customer.

3. **Data Controllers.** Data Controller provides a limited amount of its instructor and/or learner user data to Class. The parties agree that all processing of Personal Data by Class and/or any Sub-processor will be performed only pursuant to the instructions from Data Controller as set forth in the Agreement. Class understands and agrees that Data Controller has the rights and obligations as set forth in Applicable Law.
4. **Obligations of Class.** Class, to the extent it is a data processor under the terms of this DPA and applicable data protection law, agrees:
    1. to process Personal Data only under the authority of and on behalf of the written instructions of Data Controller, including as set forth in the Agreement, unless required by law to act without or against such instructions, in such case Class shall inform the Data Controller immediately of such legal requirements unless Class is legally prohibited from doing so;
    2. to ensure that any persons authorized to process Personal Data have confidentiality obligations or are under appropriate fiduciary obligations of confidentiality;
    3. all Personal Data processed by Class will be stored in regional servers around the world as applicable to Customer;
    4. that it has implemented and maintains commercially appropriate technical and organizational security measures appropriate for the nature, scope and type of processing being performed in compliance with the Applicable Law;
    5. to notify the Data Controller without undue delay after confirmed knowledge by Class of any Personal Data Breach. Class will comply with the Personal Data Breach-related obligations directly applicable to it under Applicable Law. Class will undertake steps to mitigate any Personal Data Breach and provide Data Controller information regarding: (a) the nature of the data breach; (b) the number and categories of data subjects and data records affected; and (c) the name and contact details for the relevant contact person at Class. Class will not assess the contents of Data Controller's Personal Data in order to identify information subject to any specific legal requirements. Unless otherwise indicated, Data Controller is solely responsible for complying with legal requirements for notification applicable to it and fulfilling any third-party notification obligations related to any Personal Data Breach. Nothing shall be construed to be an acknowledgement of fault or liability for such Personal Data Breach or require Class to violate, or delay compliance with, any legal obligation it may have with respect to a Personal Data Breach or other security incidents generally.
    6. to the extent Data Controller, in its use of the Services, does not have the ability to address a request regarding Personal Data directly, to provide reasonable assistance, to the extent legally permitted, to Data Controller to allow it to respond to any request by a data subject seeking to exercise any of his or her rights under Applicable Laws (including rights of access, correction, objection, and erasure, as applicable) with respect to Personal Data held by Class or its subprocessor;

7. to provide reasonable assistance to Data Controller in complying with any legally binding requests related to Personal Data by a law enforcement authority unless otherwise prohibited, including in responding to a Personal Data Breach and complying with any applicable data breach notification laws in connection with a Personal Data Breach and to provide reasonable assistance to Data Controller with data protection impact assessments and consultations, when and if required by Applicable Laws;
8. to abide by and cooperate with the requests of the supervisory authority in the EU with regard to the processing of Personal Data;
9. To the extent required by Applicable Law, to submit its data processing activities for audit by the Data Controller as required to reasonably demonstrate compliance with its obligations under no more than once annually, provided that Data Controller or any third-party representative is bound by obligations of confidentiality for such audit information. For clarity, such audits or inspections are limited to Class's processing of Personal Data on behalf of Data Controller only, not any other aspect of Class's business or information systems or other Customers. Data Controller shall provide Class with sixty (60) days prior written notice to an audit, shall conduct an audit, at Data Controller's sole expense, in a manner that will result in minimal disruption to Class's business operations and, to the extent Class's personnel are required to cooperate therewith, occur during normal business hours. Data Controller shall not be entitled to receive data or information of other Customers or any other confidential information that is not directly relevant for the authorized purposes of the audit. This provision does not grant Data Controller any right to conduct an on-site audit of Class's premises. Data Controller shall reimburse Class for any reasonable time expended for an audit at the Class's then-current rates, which shall be made available to Data Controller upon request.

5. **Sub-processors.** Data Controller acknowledges and agrees that Class may engage Sub-processors for the Processing of EU Data Subject Personal Data in compliance with Applicable Laws to provide the Services. Class will impose contractual obligations on any Sub-processors that are substantially the same as the data protection obligations set forth in this DPA and will remain liable to Data Controller for Sub-processors' performance of such data protection obligations. Class has provided a current list of Class's Sub-processors listed herein as Schedule C. Class will maintain an up-to-date list of its Sub-processors, and it will provide Data Controller with reasonable notice of any new Sub-processor added to the list. In the event Data Controller notifies Class in writing within 10 days of such notification of a new Sub-Processor of a good faith objection to a new Sub-processor based on its ability to process Personal Data in compliance with this DPA: (a) Class will provide information about such Sub-Processor to address Data Controller's concerns or (b) work in good faith to provide the Services without such Sub-Processor, if commercially feasible. Data Controller acknowledges that certain Sub-Processors are essential to the Services, and the Services cannot be provided without them. In such case, following a good faith and reasonable objection that is not addressed by this section 5(a), Data Controller may terminate the Services, at their own cost and without any claim to a refund for services rendered.
6. **Obligations of Data Controller.** Data Controller agrees and represents and warrants to Class the following:
    1.
        1. that it has obtained all necessary rights and consents under applicable data protection law as required for Class to perform the Services under the Agreement or otherwise process any Personal Data as contemplated in this DPA;
        2. Data Controller will not instruct Class to process Personal Data in violation of any applicable law. In the event of a change in the legislation that is likely to have a substantial adverse effect on the warranties and obligations provided by this DPA, Data Controller will promptly notify Class of such change, in which case Class is entitled to suspend the processing of the relevant Sub-processors; and
        3. to implement and maintain data protection policies that are compliant with the Applicable Laws.
7. **Data Transfers Outside of the EU, UK, or Switzerland.** Data Controller authorizes Class to transfer, store or Process Personal Data in the United States or any other country in which Class or its Subprocessors maintain facilities.
        1. To the extent legally required, by signing this DPA, Data Controller and Class are deemed to have signed the EU SCCs, which form part of this DPA and (except as described in Section 7(b) and (c) below) will be deemed completed as follows:
            1. Module 2 of the EU SCCs applies to transfers of Personal Data from Data Controller (as a controller) to Class (as a processor);
            2. Clause 7 (the optional docking clause) is not included;
            3. Under Clause 9 (Use of sub-processors), the Parties select Option 2 (General written authorization). The initial list of Sub-processors is set forth in Schedule C of this DPA and Class shall update that list and provide a notice to Data Controller in advance of any intended additions or replacements of Sub-processors as provided in Section 6.

4. Under Clause 11 (Redress), the optional language requiring that Data Subjects be permitted to lodge a complaint with an independent dispute resolution body shall not be deemed to be included;
5. Under Clause 17 (Governing law), the Parties choose Option 1 (the law of an EU Customer State that allows for third-Party beneficiary rights). The Parties select the laws of Ireland;
6. Under Clause 18 (Choice of forum and jurisdiction), the Parties select the courts of Ireland;
7. Annex I(A) and I(B) (List of Parties) is completed as set forth in Schedule A of this DPA;
8. Under Annex I(C) (Competent supervisory authority), the Parties shall follow the rules for identifying such authority under Clause 13 and, to the extent legally permissible, select the Irish Data Protection Commission.
9. Annex II (Technical and organizational measures) is completed with Schedule B of this DPA; and
10. Annex III (List of subprocessors) is not applicable as the Parties have chosen General Authorization under Clause 9. A list of Class's current Sub-processors is available in Schedule C

2. With respect to Personal Data transferred from the United Kingdom for which United Kingdom law (and not the law in any European Economic Area jurisdiction or Switzerland) governs the international nature of the transfer, the UK SCCs form part of this DPA and takes precedence over the rest of this DPA as set forth in the UK SCCs. Undefined capitalized terms used in this provision shall mean the definitions in the UK SCCs. For purposes of the UK SCCs, they shall be deemed completed as follows:
    1. The Parties' details shall be the Parties and their affiliates to the extent any of them is involved in such transfer;
    2. The Key Contacts shall be the contacts set forth in the Agreement, including this DPA;
    3. The Approved EU SCCs referenced in Schedule A shall be the EU SCCs as executed by the Parties;
    4. Annex 1A, 1B, II, and III shall be set forth in Schedules A, B, and C below;
    5. Either Party may end this Addendum as set out in Section 19 of the UK SCCs; and
    6. By entering into this Addendum, the Parties are deemed to be signing the UK SCCs and agree that the Addendum will be governed by the laws of England and Wales and enforced by the courts and relevant supervisory authorities in England and Wales.
3. For transfers of Personal Data that are subject to the FADP, the EU SCCs form part of this Addendum as set forth in Section 12(a) of this Addendum, but with the following differences to the extent required by the FADP:
    1. References to the GDPR in the EU SCCs are to be understood as references to the FADP insofar as the data transfers are subject exclusively to the FADP and not to the GDPR;
    2. References to personal data in the 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;
    3. The term "Customer state" in EU SCCs 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 EU SCCs; and
    4. The relevant supervisory authority is the Swiss Federal Data Protection and Information Commissioner (for transfers subject to the FADP and not the GDPR), or both such Commissioner and the supervisory authority identified in the EU SCCs (where the FADP and GDPR apply, respectively).

8. **Return or Destruction of Personal Data.** Except to the extent required otherwise by Applicable Laws, Class will, at the choice of Data Controller and upon Data Controller's written request, either at the termination of the Agreement or at any time during the term of the Agreement, return to Data Controller and/or securely destroy all Personal Data. Except to the extent prohibited by Applicable Laws, Class will inform Data Controller if it is not able to return or delete the Personal Data.
9. **Liability**
    1. The parties agree that nothing herein in this DPA or the Agreement relieves the Customer of its respective responsibilities and liabilities under applicable data protection law.

2. Each party's liability towards the other party under or in connection with this DPA will be limited in accordance with the provisions of the Agreement.
3. Customer acknowledges that Class is reliant on Customer for direction as to the extent to which Class is entitled to process Personal Data on behalf of Customer in performance of the Services. Consequently, Class will not be liability under the Agreement for any claim brought by a data subject arising from any action or omission by Class, to the extent that such action or omission resulted from Customer's instructions or from Customer's failure to comply with its obligations under applicable data protection law. **The parties agree that the liability of Class shall be limited to its own processing operations under this DPA and the Agreement. The parties agree that Class will not be liable for any damages arising out of or related to violations of applicable data protection law by the Data Controller related to Data Controller's acts or omissions not related to the Services.**

10. **Ratification.** All other terms and conditions in the Agreement are ratified and remain in full force and effect. This DPA is an addendum to the Agreement and shall control and prevail to the extent of any conflict with the Agreement. In the event of a conflict between this DPA and the EU SCCs or UK SCCs, the terms of the EU SCCs or UK SCCs, as relevant, will control.
11. **Survival.** The provisions of this DPA survive the termination or expiration of the Agreement for so long as Class or its Sub-processors Process the Personal Data.

Schedule A

ANNEX I

1. LIST OF PARTIES

Data exporter(s):

Name: The exporter (Controller) is Data Controller and Data Controller's contact details and signature are as provided in the Agreement and the DPA.

Activities relevant to the data transferred under these SCCs: The data exporter is a user of Class's Services pursuant to their underlying Agreement. The data exporter acts as a controller with respect to its own personal data.

Signature and date: The Parties agree that execution of the Agreement shall constitute execution of these SCCs by both Parties.

Data importer(s):

Name: The importer (Processor) is Class and Class's contact details and signature are as provided in the Agreement and the DPA.

Activities relevant to the data transferred under these SCCs: The data importer is the provider of Services to the data exporter and its customers pursuant to their underlying Agreement. The data importer acts as the data exporter's processor.

Signature and date: The Parties agree that execution of the Agreement shall constitute execution of these SCCs by both Parties.

a. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred: Data Controller's employees and authorized users.

Categories of personal data transferred: Any personal data provided by Data Controller to Class for Class to perform services under the underlying Agreement and the DPA.

Sensitive data transferred (if applicable): N/A

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis): On a continuous basis as needed to provide the Services to Data Controller.

Nature of the processing: The nature of the processing is set out in the Agreement between the parties

Purpose(s) of the data transfer and further processing: The purposes of the data transfer is to provide the Services chosen by Data Controller in connection with the Agreement.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: The data will be retained for the time period needed to accomplish the purposes of Processing, unless otherwise required by applicable law.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing: Same as above to the extent such information is provided to Sub-processors for purposes of providing the Services.

a. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13: The data exporter's competent supervisory authority will be determined in accordance with the GDPR, and where possible, will be the **Irish Data Protection Commissioner**.

Schedule B

DATA SECURITY MEASURES

The Parties will implement and maintain the following administrative, technical, physical, and organizational security measures for the Processing of Personal Data:

Parties' Information Security Program includes specific security requirements for its personnel and all subprocessors or agents who have access to Personal Data ("Data Personnel"). The security program covers the following areas:

1. Information Security Policies and Standards. The Parties will maintain written information security policies, standards and procedures addressing administrative, technical, and physical security controls and procedures. These policies, standards, and procedures shall be kept up to date, and revised whenever relevant changes are made to the information systems that use or store Personal Data.
2. Physical Security. The Parties will maintain commercially reasonable security systems at all Party sites at which an information system that uses or stores Personal Data is located ("Processing Locations") that include reasonably restricting access to such Processing Locations, and implementing measures to detect, prevent, and respond to intrusions.
3. Organizational Security. The Parties will maintain information security policies and procedures addressing acceptable data use standards, data classification, and incident response protocols.
4. Network Security. The Parties maintains commercially reasonable information security policies and procedures addressing network security.
5. Access Control. The Parties agree that: (1) only authorized staff can grant, modify or revoke access to an information system that Processes Personal Data; and (2) the Parties will implement commercially reasonable physical and technical safeguards to create and protect passwords.
6. Virus and Malware Controls. The Parties protect Personal Data from malicious code and will install and maintain anti-virus and malware protection software on all system endpoints that handle Personal Data and will maintain applicable controls on web servers.
7. Personnel. The Parties have implemented and maintains a security awareness program to train employees about their security obligations. Data Personnel follow established security policies and procedures. Disciplinary process is applied if Data Personnel fail to adhere to relevant policies and procedures.
8. Business Continuity. The Parties implement disaster recovery and business resumption plans that are kept up to date and revised on a regular basis. The Parties also adjust the Information Security Program in light of new laws and circumstances, including as business and Processing change.
9. Specific details are provided at the Class Trust Center, located at https://trust.class.com/

Schedule C
CLASS SUBPROCESSORS

A list of Class's current Sub-processors is available at the following link: https://trust.class.com/.