Data Processing Addendum | Policy 2022

This Instructure Data Processing Addendum ("**DPA**") forms part of the Instructure Services Order Form and Instructure Standard Terms and Conditions, or other written or electronic agreement ("**Agreement**") between Customer Instructure, Inc., or its Affiliates (collectively "**Instructure**") (each a "**Party**", collectively "**Parties**"). The Parties hereby agree that the terms and conditions set out below shall be added as an addendum to the Agreement. In case of any discrepancy or conflict between this DPA and the Agreement, this DPA shall prevail. In case of any discrepancy between this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail. Any capitalized terms not defined herein shall have the meanings set forth in the Agreement.

How this DPA Applies: Instructure provides the Services (as defined in the Agreement) to Customer which may include the Processing of Personal Data by Instructure during the provision of the Services. This DPA does not replace any rights related to the Processing of Customer Personal Data previously negotiated by Customer in the Agreement. Instructure agrees to comply with this DPA with respect to any Customer Personal Data Processed by Instructure in the provision of the Services under applicable Data Protection Laws.

1. **DEFINITIONS.** In this DPA, the following terms shall have the meanings set out below:
    1. "**Affiliates**" means any entity which is controlled by, controls or is in common control with a Party.
    2. "**Customer Personal Data**" means Personal Data provided by or on behalf of Customer to be Processed by Instructure in connection with providing the Services.
    3. "**Data Controller**" means the entity which determines the purposes and means of the Processing of Personal Data.
    4. "**Data Processor**" means the entity which Processes Personal Data on behalf of the Data Controller.
    5. "**Data Protection Laws**" means the laws and regulations which are applicable to the Processing of Personal Data under the Agreement.
    6. "**Data Subject**" means an individual whose Personal Data is being processed by the Data Processor under the Agreement.
    7. "**EEA**" means the European Economic Area, consisting of the Member States of the European Union and Iceland, Liechtenstein, and Norway.

8. “**GDPR**” means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC and the UK equivalent.
9. “**Personal Data**” means any information relating to an identified or reasonably identifiable person.
10. “**Processing**” means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction (“**Process**”, “**Processes**” and “**Processed**” shall have the same meaning).
11. “**Sell,**” “**Selling**,” “**Sale**,” and “**Sold**” shall have the meanings provided under applicable Data Protection Laws.
12. “**Security Breach**” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, the Personal Data transmitted, stored, or otherwise processed by Instructure.
13. **“Standard Contractual Clauses**” means the contractual clauses issued by the European Commission by implementing decision 2021/914 of 4th of 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 Council, the UK International Data Transfer Addendum (“**UK Addendum**”), and any similar measures promulgated pursuant to the GDPR to address the transfer of Personal Data to a Third-country and any amendments and replacements thereto as may be promulgated from time to time.
14. “**Supplementary Measures**” means technical, organizational, and contractual measures as described in EDPB Guideline adopted on 18th June 2021 (“Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data”).
15. “**Sub-processor**” means any Data Processor acting on behalf of Instructure.

16. “**Third-country**” means a country that is neither part of the EEA nor has been declared adequate by a decision of the European Commission according to the mechanism lined out in Article 45 GDPR.

17. “**UK**” means the United Kingdom, Wales, and Northern Ireland.

2. **PROCESSING OF CUSTOMER PERSONAL DATA.**

    1. The Parties agree that with regard to the Processing of Customer Personal Data, Customer is the Data Controller and Instructure is the Data Processor, except for certain services provided by Instructure where Instructure is also a Data Controller with respect to the Customer Personal Data.

    2. Customer shall, in its use or receipt of the Services, process Customer Personal Data in accordance with the requirements of the Data Protection Laws and Customer will ensure that its instructions for the Processing of Customer Personal Data comply with the Data Protection Laws. Customer shall have sole responsibility for the accuracy, quality, and legality of Customer Personal Data, the means by which Customer obtained the Customer Personal Data, and for fulfilling all requirements under Data Protection Laws necessary to make the Customer Personal Data available to Instructure for Processing as provided herein and under the Agreement.

    3. During the Term of the Agreement, Instructure shall only Process Customer Personal Data on behalf of and in accordance with the Agreement and Customer’s written instructions unless required to do so by law to which Instructure is subject; in such case Instructure shall inform the Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

    4. Customer instructs Instructure to Process Customer Personal Data for the following limited and specified purposes: (i) Processing in accordance with the Agreement, any applicable orders, and Data Protection Laws; and (ii) Processing to comply with other reasonable instructions provided by Customer where such instructions are consistent with the terms of the Agreement and Data Protection Laws. Instructure shall not Sell, or share for targeted advertising purposes, Customer’s Personal Data except as expressly instructed by Customer. Instructure shall not combine Customer Personal Data with other Personal Data except as permitted by Data Protection Laws.

5. The objective of Processing of Customer Personal Data by Instructure is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Appendix 1, Annex I B.
6. If Instructure determines that it can no longer comply with Data Protection Laws, Instructure will notify Customer within five (5) business days of making such determination.

3. **ASSISTANCE TO CUSTOMER AND RIGHTS OF DATA SUBJECTS.**
    1. To the extent Customer, in its use or receipt of the Services, does not have the ability to take steps required to comply with Data Protection Laws, including without limitation correcting, amending, restricting, blocking or deleting Customer Personal Data, and implementing reasonable security procedures or practices designed to protect Customer Personal Data, as and to the extent required by the Data Protection Laws, Instructure will use commercially reasonable efforts to comply with reasonable requests by Customer to facilitate such actions to the extent Instructure is legally permitted to do so, taking into account the nature of the Processing of Customer Personal Data and the information available to Instructure.
    2. Instructure shall, to the extent legally permitted, promptly notify Customer if it receives a request from a Data Subject for access to, correction, amendment, deletion of or objection to the processing of that person's Personal Data. Instructure shall not respond to any such Data Subject request without Customer's prior written consent except to confirm that the request relates to Customer or as otherwise required by Data Protection Laws. Instructure shall provide Customer with commercially reasonable cooperation and assistance in relation to the handling of a Data Subject's request, to the extent legally permitted and to the extent Customer does not have access to such Customer Personal Data through its use or receipt of the Services, taking into account the nature of the Processing of Customer Personal Data and the information available to Instructure.

4. **PROCESSOR PERSONNEL.**
    1. Instructure shall use commercially reasonable efforts to ensure that its personnel engaged in the Processing of Customer Personal Data are subject to obligations of confidentiality.

2. Instructure shall use commercially reasonable efforts to ensure that access to Customer Personal Data is limited to those personnel who require such access to perform the Services.

5. **SUB-PROCESSORS.**

    1. Instructure shall not transfer or otherwise make available Customer Personal Data to any third party without Customer's prior authorization.

    2. Upon signing of the DPA, Customer gives its general authorization to Instructure to use Instructure Affiliates as Sub-processors; and third-party Sub-processors in connection with the provision of the Services provided that the following conditions are met:

        1. Instructure shall ensure that obligations not materially less protective than those set out in this DPA are imposed on Sub-processors by way of a written contract;

        2. Instructure remains liable towards Customer for the work of its Sub-processors as if and to the extent such work was performed by Instructure;

        3. Instructure shall provide the list of its Sub-processors by giving a link to a website where the information about the Sub-processors is kept up to date; and

        4. Instructure shall inform Customer of any intended changes to Sub-processors concerning the addition or replacement of Sub-processors. To the extent required by Data Protection Laws, Instructure shall thereby give Customer the opportunity to object to such changes by notifying Instructure in writing within 30 days after the receipt of Instructure's notice about the changes, and if, within 20 days of receipt of that notice, Customer notifies Instructure in writing of any objections on reasonable grounds to the proposed engagement of a Sub-processor, Instructure shall not use that proposed Sub-processor to Process Customer Personal Data until reasonable steps have been taken to address the objections raised by Customer and Customer has been provided with a reasonable written explanation of the steps taken.

6. **INTERNATIONAL DATA TRANSFERS**

    1. Customer acknowledges and agrees that Instructure is established in a Third Country and that providing the Services defined in the Agreement require transfer to, and Processing of Customer Personal Data within, a

Third Country. All transfers to a Third Country are subject to the following conditions:

1. Customer has given prior authorization for the transfer by signing the Agreement as documented in Appendix 1;
2. The Customer Personal Data is Processed under the terms of the Agreement;
3. There is a valid transfer mechanism in place in accordance with the GDPR; and
4. Instructure shall implement the Supplementary Measures, where necessary.

2. **EU/UK Standard Contractual Clauses:** The valid transfer mechanism referred in Section 6.1(iii) is, where Instructure acts as a Processor and Customer acts as a Controller, the Standard Contractual Clauses, Module TWO: Transfer Controller to Processor; where Instructure acts as a Controller and Customer acts as a Controller, the Standard Contractual Clauses, Module ONE: Transfer Controller to Controller; and in both cases, the UK Addendum thereto attached as Appendix 2, and all of the foregoing are deemed to be incorporated herein by reference as set forth below. In respect of the Standard Contractual Clauses, the Parties agree on the following:
    1. in clause 7, the Parties choose to include the “docking clause”;
    2. where Module Two applies, in clause 9, the Parties choose Option 2: “general written authorization”;
    3. where Module Two applies, in clause 9, the Parties choose twenty (20) days as the specific time period;
    4. in clause 11, the Parties do not choose the optional complaint mechanism;
    5. in clause 17, the governing law is the law of the EU Member State :
        1. Option 1: Where Customer is established in an EU Member State, the law in that EU Member State;
        2. Option 2: Where Customer is not established in an EU Member State but has appointed a representative pursuant to Article 27(1) of the GDPR, the law in the EU Member State in which the Customer’s representative is located;

3. Option 3: Where the data exporter is not established in an EU Member State and is not required to appoint a representative pursuant to Article 27(2) of the GDPR, the law of Hungary, or as defined in the Agreement; and

6. in clause 18, the country of the applicable court in respect of any disputes arising from Standard Contractual Clauses is the courts of the EU Member State in which in which the Parties have denoted choice of law per 6.2(v) above.

3. To the extent that Instructure uses a Sub-processor in a Third-Country for the Processing of Customer Personal Data, the following shall apply in addition to **Section 5** above:

    1. Customer has given prior authorization for the transfer by signing the DPA;

    2. There is a valid transfer mechanism in place in accordance with the GDPR; and

    3. Instructure makes information on the transfer mechanism, and where applicable, the Standard Contractual Clauses, available without undue delay to Customer.

7. **SECURITY; AUDIT RIGHTS; PRIVACY IMPACT ASSESSMENTS.**

    1. Instructure shall maintain technical and organizational measures designed to protect of the security, confidentiality, and integrity of Customer Personal Data.

    2. No more than once per year, Customer may engage a mutually agreed upon third party to audit Instructure solely for the purposes of meeting its audit requirements pursuant to the Data Protection Laws. To request an audit, Customer must submit a detailed audit plan at least four (4) weeks in advance of the proposed audit date describing the proposed scope, duration, and start date of the audit. Audit requests must be sent to privacy@Instructure.com. The audit must be conducted during regular business hours, subject to Instructure's policies, and may not unreasonably interfere with Instructure's business activities. Any audits are at Customer's expense.

    3. Any request for Instructure to assist with an audit is considered a separate service if such audit assistance requires the use of resources different from or in addition to those required by law. Customer shall reimburse Instructure for any time spent for any such audit at the rates agreed to by

the Parties. Before the commencement of any such audit, Customer and Instructure shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which Customer shall be responsible. All reimbursement rates shall be reasonable, considering the resources expended by Instructure. Customer shall promptly notify Instructure with information regarding any non-compliance discovered during an audit.

4. Instructure will reasonably cooperate with Customer, at Customer's expense, where Customer is conducting a privacy impact assessment that is required by Data Protection Laws.

8. **SECURITY BREACH MANAGEMENT AND NOTIFICATION.**

    1. In the event of a Security Breach, Instructure shall: (i) notify Customer of the Security Breach without undue delay after becoming aware of the Security Breach. Notification shall include at least the information required by the Data Protection Laws; (ii) investigate the Security Breach and provide Customer with information about the Security Breach; and (iii) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Breach and to allow Customer to take reasonable and appropriate steps to do the same to the extent such steps are within Customer's control.

    2. Instructure shall cooperate with Customer, and with any third parties designated by Customer, to respond to the Security Breach.

9. **RETURN AND DELETION OF CUSTOMER DATA.**

    1. Instructure shall provide functionality for Customer to download Customer Personal Data from the Services, to the extent possible, and/or delete Customer Personal Data in accordance with Instructure's data retention policies which adhere to requirements of the Data Protection Laws, and in a manner consistent with the terms of the Agreement.

10. **SEVERANCE.**

    1. Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or, if this is not possible, construed in a manner as if the invalid or unenforceable part had never been contained therein.

11. **LEGAL EFFECT.**

1. This DPA shall only become legally binding between Customer and Instructure when the Parties the Agreement for the Services.

12. **LIMITATION OF LIABILITY.**

    1. To the extent permitted by Data Protection Laws, Customer's remedies with respect to any breach by Instructure of the terms of this DPA or Data Protection Laws will be subject to any aggregate limitation of liability that applies to Instructure and/or Customer under the Agreement.