Data Processing Addendum

The terms of this Data Processing Addendum ("**DPA**") are incorporated by reference to the Master Agreement between you and Transact ("Transact" "we", "us" and "our") (the "**Agreement**"). By agreeing to the terms of this DPA, you and Transact are agreeing to abide by the various data protection laws (as defined below) applicable to the processing of personal information in the jurisdictions where you and Transact are located or doing business. Capitalized terms not herein defined shall have the same meanings in the Agreement.

In the course of providing services under the Agreement, Transact may process certain personal information on behalf of Customer ("**Customer Data**") and where Transact processes such personal Information on behalf of Customer and Transact and Customer agree to comply with the terms and conditions in this DPA in connection with such Customer Data.

Data Processing Clauses

The following provisions shall apply whenever Customer Data are processed on your behalf:

1. Definitions

1.1 "Customer Personal Data" means any Personal Data Processed by a Contracted Processor on behalf of the Customer pursuant to or in connection with the Principal Agreement.

1.2 "Contracted Processor" means Transact or a Subprocessor.

1.3 "Data Breach" means a breach of Transact's security measures leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data.

1.4 "Data Protection Laws" means, as applicable: (a) EU Data Protection Laws; (b) US Data Protection Laws; and (band (c) any other laws, rules, regulations, self-regulatory guidelines, implementing legislation, or third party terms relating to privacy, security, breach notification, data protection, or confidentiality and applicable to processing of personal information.

1.5 "European Data Protection Laws" means: (i) the EU GDPR; (ii) the UK GDPR; (iii) the EU e-Privacy Directive 2002/58/EC; and (iv) any and all applicable national data protection laws made under, pursuant to or that apply in conjunction with any of (i), (ii) or (iii); in each case as may be amended or superseded from time to time.

1.6 "EU GDPR" means EU General Data Protection Regulation 2016/679.

1.7 "Personal Information" means any information relating to an identified or identifiable natural person, or that relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular natural person or household. Personal Information includes Non-Public Personal Information, Personal Data, Personal Digital Identifiers, Personal Information, Personally Identifiable Information, and any other information defined by similar term under Data Protection Laws.

1.8 "Restricted Transfer" means:

(a) a transfer of Customer Personal Data from Customer to a Contracted Processor; or
(b) an onward transfer of Customer Personal Data from a Contracted Processor to a Contracted Processor, or between two establishments of a Contracted Processor,

in each case:

(c) where the EU GDPR applies, such transfer of Customer Personal Data is to a country outside of the European Economic Area which is not subject to an adequacy determination by the Commission; and

(d) where the UK GDPR applies, such transfer of Customer Personal Data is to a country outside of the United Kingdom which is not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018; or

(e) where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws) in the absence of the Standard Contractual Clauses to be established below.

1.9 "Standard Contractual Clauses" means (1) where the EU GDPR applies, the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 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 the Council, which can be found on the European Commission's website ("EU SCCs"); and (ii) where the UK GDPR applies, standard data protection clauses adopted pursuant to or permitted under Article 46 of the UK GDPR ("**UK SCCs**").

1.10 "Subprocessor" means any person (including any third party and any Transact Affiliates, but excluding an employee of Transact or any of its sub-contractors) appointed by or on behalf of Transact or any Transact Affiliate to Process Customer Personal Data on behalf of the Customer in connection with the Principal Agreement;

1.11 "UK GDPR" means the EU GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018;

1.12 "US Data Protection Laws" means the data protection and privacy laws of the United States and each of its states and territories including, without limitation, (a) the California Consumer Privacy Act of 2018 (“CCPA”), the California Privacy Rights Act of 2020 ("CPRA"), the Colorado Privacy Act ("CPA"), the Connecticut Data Privacy Act ("CDPA"), the Utah Consumer Privacy Act ("UCPA"), and the Virginia Consumer Data Protection Act ("VCDPA").

1.13 The terms, "Commission", "Controller", "Data Subject", "Personal Data", Processor", "Processing" and "Supervisory Authority" shall have the same meaning as in the European Data Protection Laws. The terms, "Business Purpose", "Sell", and "Service Provider", shall have the same meaning as in the US Data Protection Laws. With respect to the US Data Protection Laws, the term Personal Data means and includes Personal Information as defined in the US Data Protection Laws.

2. Transact and Customer obligations

2.1 We shall process Customer Data and information provided by you or your Authorized End Users within the scope of the Agreement, for the purpose of service provision during the term of the Agreement, and pursuant to your documented instructions (unless required to process Customer Data other than instructed by applicable law, in which case we will, before processing Customer Data in accordance with that law, inform you unless that law prohibits us from doing so). You warrant your collection and sharing of Customer Data with us and our processing of Customer Data solely in accordance with the Agreement shall comply with Data Protection Laws and that all Personal Information provided to Transact has all authorizations and/or consents necessary to provide such Personal Information to Transact. We shall not compile copies or duplicates without your approval, except for copies made for backup or disaster recovery purposes. We shall only process Personal Information on our systems or in our facilities to the extent necessary to perform our obligations under the Agreement. You shall keep the amount of Personal Information provided to Transact to the minimum necessary for the provision of products and services by Transact pursuant to the Agreement.

2.2 Annex A of this DPA contains a list of the categories of Customer Data, the data subjects concerned, the nature and purpose of processing.

3. Data Subject Requests; Authority to issue instructions

3.1 Transact shall, to the extent legally permitted, promptly redirect the data subjects to send their requests to the you or notify you if it receives a request from a data subject for access to, rectification, portability, objection, restriction or erasure of such data subject's Personal Information. Unless required by Data Protection Laws, Transact shall not respond to any such data subject request without your prior written consent except to redirect the data subject to the you. Transact shall provide such information and cooperation and take such action as the you reasonably requests in relation to a data subject request.

3.2 We agree, without limitation, to strictly follow any instructions given by you under the Agreement as well as those issued on an individual basis regarding the collection, processing and/or usage of Customer Data. This includes but is not limited to instructions on the blocking, correction or deletion of Customer Data. Our obligations under this Section 3.2 shall be subject to Section 3.4.

3.3 Instructions may only be issued by your authorized officers, data protection officers or the manager of your legal department, if applicable ("Authorized Persons"). The Authorized Persons shall have the right to make written appointments of additional other Authorized Persons.

3.4 You warrant that you shall give only lawful instructions conforming to applicable Data Protection Laws. If we hold the view that any instruction of yours contravenes Data Protection Laws and/or the Agreement, we will notify you, and we are entitled to suspend execution of the instruction concerned, until you confirm such instruction in writing. We have the right to deny the execution of an instruction – even if issued in writing – in case we conclude that we would be liable under Data Protection Laws if we execute the instructions you have provided.

4. Data Security

4.1 We undertake to maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Customer Data), pursuant to applicable Data Protection Laws, and keep Customer Data confidential. We will ensure that such persons with access to Customer Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

4.2 We agree that we make our applicable employees familiar with the relevant provisions of the Data Protection Laws and shall provide adequate training. We shall supervise compliance of such employees with applicable Data Protection Laws.

5. Sub-Processing

5.1 In accordance with the provisions of this DPA and the Agreement, you acknowledge and agree that Transact, Transact affiliates ("Transact Affiliates") or other sub-processors engaged to provide the Services provided (which are hereby designated as sub-processors for the purpose of processing Customer Data) may store or process Customer Data in various data centers around the world and that Customer Data might not be hosted within the country in which you are located provided that (a) notwithstanding any notice requirement in the Agreement, we shall not engage a sub-processor processing Customer Data without your authorization and give you an opportunity to review such engagement and reasonable time to make any objection to such changes (we may provide notice via electronic communication or published on our website); and (b) the sub-processors processing Customer Data are subject to the same data protection obligations or the same level of protection as are contained in the DPA. Customer agrees to raise any reasonable objections in writing within ten (10) business days such notification. You confirm that Section 5.3. constitutes general written authorization for the purposes of GDPR. We shall remain liable for any processing of Customer Data carried out by sub-processors engaged under the Agreement. Upon your request, we will tell you where Customer Data is located. Notwithstanding anything to the contrary in this Section, if we and you have agreed that Customer Data will be stored in any particular location, we will store such Customer Data in the agreed location.

5.2 You acknowledge and agree that Transact may transfer Customer Data to any country outside the European Economic Area ("**EEA**") or to any country which has not been the subject of a European Commission adequacy decision provided such a transfer is made pursuant to an appropriate legal transfer mechanism, such as any replacement to the EU-US Privacy Shield Framework, the EU Commission Model Standard Clauses or any other legal transfer mechanism. To the extent that the legal transfer mechanism relied on is declared invalid (by, for example, a competent court or authority), Transact shall cooperate with Customer in good faith to find an alternative legal transfer mechanism.

5.3 For the purposes of Clause 9 of the Standard Contractual Clauses, you provide a general consent to Transact to engage sub-processors. Such consent is conditional on Transact's compliance with Section 5 of this DPA.

6. Audit

6.1 Transact has obtained third-party certifications and audits and upon Customer's request shall make these reports available to Customer. Transact shall make available to Customer information regarding Transact's compliance with the obligations set forth in this DPA.

6.2 You have the right to audit our compliance with the Data Protection Laws and the stipulations entered into between the Parties (including the technical and organizational measures), by requesting information about and reasonably inspecting storage of the Customer Data, and implemented policies and security incident reports, subject to reasonable prior notice of at least ten (10) business days in advance and, to the extent reasonably possible, without interfering with our regular business operations. Customer and Transact shall mutually agree upon the scope, timing and duration of the audit, the cost of which shall be borne by Customer.

6.3 Upon your request, Transact shall provide reasonable cooperation needed to fulfill Customer's obligations under the GDPR to carry out a data impact assessment related to Customer's use of the services, to the extent that Customer does not otherwise have access to the information requested, and to the extent such information is available to Transact. Transact shall provide reasonable assistance and cooperation to Customer in these circumstances.

6.4 Customer agrees that, taking into account the nature of the processing of Customer Data under the Agreement, by providing the assistance and information contained in this Agreement, we have assisted you in ensuring compliance with your obligations in respect of data protection impact assessments and prior consultation under Articles 35 and 36 of the GDPR.

7. Security Incident Management

7.1 In accordance with the Data Protection Laws and other industry standards, Transact has appropriate policies and procedures in place to manage a Data Breach.

7.2 In accordance with the Data Protection Laws, Transact shall notify you without undue delay in the event of a Data Breach relating to Customer Data, of which Transact reasonably suspects or knows to have occurred, and which requires a notification to be made to a supervisory authority under the applicable Data Protection Laws. Transact shall provide commercially reasonable cooperation and assistance in identifying the cause of the Data Breach and take all commercially reasonable steps to remediate the Data Breach to the extent within Transact's control.

7.3 You agree that, given the nature of the processing, Section 7 satisfies our obligation to assist you with your obligations under Articles 33 and 34 of the GDPR.

7.4 In addition, we shall notify you reasonable notice about:

(a) any legally binding request for disclosure of the Customer Data by a law enforcement authority or other organization or body, unless prohibited by law; and

(b) any request received directly by us from a data subject or other deletion request. Taking into account the nature of the processing activities, Transact shall reasonably cooperate with Customer to fulfill Customer's obligation to respond to any individual's request for data deletion, and such rights are afforded to the individual under the Data Protection Laws. To the extent legally permitted Customer shall be responsible for any reasonable costs or fees associated with responding to such requests.

8. Deletion of Data

8.1 Upon expiration or earlier termination of the processing services, or such earlier time as you request, we agree, at your request, to:

(a) return to you or your designee; or
(b) securely destroy or render unreadable or undecipherable, the relevant Customer Data in our possession, custody or control.

8.2 We shall ensure from an organizational perspective that Customer Data can be deleted within a reasonable time frame consistent with your request or deletion requirements established in the Agreement, except that we shall not be obliged to delete Customer Data from archival and back-up files except as in line with our company data deletion schedule as permitted under Data Protection Laws. If you request deletion of Customer Data in archival and back-up-files, you shall bear the costs including costs for business interruptions associated with such request.

9. Final Provisions

9.1 Unless specifically stipulated to the contrary by Customer and Transact, the duration of the commissioned data processing specified by this DPA shall be coterminous with the term of the Agreement.

9.2 Notwithstanding any notice requirements in the Agreement, we may update this DPA from time to time to better reflect changes to the law, new regulatory requirements or improvement to the service. If any update to the DPA materially affects your use of the service or your rights herein, we will provide 30 calendar days' prior notice or in-product notification. Your continued use of the service shall constitute acceptance to be bound by the updated DPA.

9.3 In the event of a conflict between this DPA and any other provision of the Agreement between you and us, this DPA will prevail; provided that if you and we have agreed in an Order Form or other customer agreement to any terms that are different from this DPA, the terms in such Order Form or customer agreement will prevail.

10. California and US Specific Provisions

10.1 This section applies to the extent that Transact processes Customer Data subject to the CCPA, the CPRA, the VCDPA, the CPA and other similar US privacy laws (the "US Privacy Laws").

10.2 Transact and Customer acknowledge and agree that Transact is a "service provider" and may receive personal information pursuant to the business purpose of providing services to Customer in accordance with the Agreement. For the avoidance of doubt, Transact shall not (i) sell personal information of Customer or any end user of Customer; (ii) retain, use, or disclose personal information for any purpose other than for the specific purpose of performing the services, including retaining, using or disclosing personal information outside of the direct business relationship between Transact and Customer. Transact acknowledges its obligations under the US Privacy Laws and shall comply with all requirements of the US Privacy Laws to the extent applicable to Transact and its products and services.

11. Transfers of Personal Data

11.1 The parties agree that when the transfer of Customer Personal Data from Customer to Transact or a Transact Affiliate is a Restricted Transfer it shall be subject to the appropriate Standard Contractual Clauses as follows:

(a) in relation to Customer Personal Data that is protected by the EU GDPR, the EU SCCs will apply completed as follows:

(i) Module Two will apply to the extent that Customer is a Controller of the Customer Personal Data;
(ii) in Clause 7, the optional docking clause will apply;
(iii) in Clause 9, Option 2 will apply, and the time period for prior notice of Subprocessor changes shall be 30 days;
(iv) in Clause 11, the optional language will not apply;
(v) in Clause 17, Option 1 will apply, and the EU SCCs will be governed by the law of the jurisdiction of the Competent Supervisory Authority set forth in Annex A;
(vi) in Clause 18(b), disputes shall be resolved before the courts of the of the jurisdiction of the Competent Supervisory Authority set forth in Annex A.
(vii) Annex I of the EU SCCs shall be deemed completed with the information set out in Annex I to this Addendum;
(viii) Annex II of the EU SCCs shall be deemed completed with the information set out in Annex II to this Addendum; and

(b) in relation to Customer Personal Data that is protected by the UK GDPR, the UK SCCs will apply completed as follows:

(i) for so long as it is lawfully permitted to rely on standard contractual clauses for the transfer of personal data to processors set out in the European Commission's Decision 2010/87/EU of 5 February 2010 ("Prior C2P SCCs") for transfers of Customer Personal Data from the United Kingdom, the Prior C2P SCCs shall apply between the Customer on the one hand and Transact or the applicable Transact Affiliate on the other hand, on the following basis:

(A) Appendix 1 shall be completed with the relevant information set out in Annex I to this Addendum;
(B) Appendix 2 shall be completed with the relevant information set out in Annex II to this Addendum; and

(ii) the optional illustrative indemnification Clause will not apply.

(c) Where section 11.1(b)(i) above does not apply, but the Customer and Transact or the applicable Transact Affiliate are lawfully permitted to rely on the EU SCCs for transfers of personal data from the United Kingdom subject to completion of a "International Data Transfer Addendum to the EU Commission Standard Contractual Clauses" ("UK Addendum") issued by the Information Commissioner's Office under s.119A(1) of the Data Protection Act 2018 and effective as of March 21, 2022, then:

(i) The EU SCCs, completed as set out above in section 11.1(a) of this Addendum shall also apply to transfers of such Customer Personal Data, subject to section 11.1(c)(ii) below;
(ii) The UK Addendum shall be deemed executed between the transferring Customer and Transact or the applicable Transact Affiliate, and the EU SCCs shall be deemed amended as specified by the UK Addendum in respect of the transfer of such Customer Personal Data.

(d) If neither section 11.1(c)(i) or section 11.1(c)(ii) applies, then the Customer and the Transact or the applicable Transact Affiliate shall cooperate in good faith to implement appropriate safeguards for transfers of such Customer Personal Data as required or permitted by the UK GDPR without undue delay.

11.2 Neither Transact nor any Transact Affiliate shall participate in (nor permit any Subprocessor to participate in) any other Restricted Transfers of Data (whether as an exporter or an importer of the Customer Personal Data) unless the Restricted Transfer is made in full compliance with European Data Protection Laws and pursuant to Standard Contractual Clauses implemented between the relevant exporter and importer of the Data.

Last Updated: December 22, 2022

Annex A – Details of the Data Processing

Controller/Data Exporter

Name: *The entity identified as the customer in the Agreement.*
Address: *The address for the customer set out in the Agreement.*
Contact Information: Name: Position: Contact Details:
Activities relevant to the data transferred under these clauses: *The receipt of services as set out in the Agreement.*
Signature and Date: *This Annex A shall be deemed executed upon the execution of this DPA.*
Role (controller/processor): *Controller*

Processor/Data Importer

Name: *The entity identified as Transact in the Agreement.*
Address: *The address for the Transact set out in the Agreement.*
Contact Information: Name: Position: Contact Details:
Activities relevant to the data transferred under these clauses: *The receipt of services as set out in the Agreement.*
Signature and Date: *This Annex A shall be deemed executed upon the execution of this DPA.*
Role (controller/processor): *Processor*

Categories of Data

Name or unique identifiers
Personal contact information including username, first name, middle name, last name, student ID, one optional demographic field.

Date of birth, Gender, Nationality, Parent/Student Relationships
Grade Level, Teachers, Classes/Sections/Courses, Grades, Assignments, Tests, Books, Attendance, Homework, Degree Type
Financial details
Usernames, passwords and credential values.
Transaction data including transaction location, type, amount, and credential used.
Service or browsing history, location data, usage history, information provided by social networks, User or Customer Correspondence
Disciplinary and conduct records
Any information contained in the submitted paper, assignment, or other user-generated content

Special Categories of Data (if any)

Information relating to disability and health
Information relating to racial or ethnic origin

Categories of Data Subject:

Customer and Customer's Users authorized by Customer to use the Transact Services (Students, Teachers and Administrators)

Frequency of Transfer:

Occurring on a continuous basis for the length of the Agreement.

Retention Period:

Customer Personal Data will be retained for the period in which services are provided under the Agreement. The criteria used to determine that period will be based on the purposes for which the data is processed and any period required to meet legal obligations or to exercise, defend or establish legal rights.
Data transferred to sub-processors will be retained for the period in which such sub-processor provides services under the Agreement. The criteria used to determine that period will be based on the purposes for which the data is

processed and any period required to meet legal obligations or to exercise, defend or establish legal rights.

Nature of Processing:

We shall process data and information provided by you or your Authorized End Users within the scope of the Agreement, for the purpose of service provision during the term of the Agreement, and pursuant to your documented instructions (unless required to process Customer Data other than instructed by applicable law, in which case we will, before processing Customer Personal Data in accordance with that law, inform you unless that law prohibits us from doing so).

Competent Supervisory Authority:

For Personal Data protected under the EU GDPR: Where the data exporter is established in the EEA, the competent supervisory authority shall be the lead supervisory authority for the data exporter. Where the data exporter is not established in the EEA but has appointed an EU representative, this shall be the supervisory authority for the territory in which the EU representative is established. In all other cases, the Data Protection Commission of the Netherlands shall be deemed the competent supervisory authority for these Standard Contractual Clauses.

For Personal Data protected under the UK GDPR: Information Commissioner's Office.

List of Sub-Processors:

The controller has authorised the use of the sub-processors made available to controller via the Client Connect Portal.

Should Customer obtain additional products or services governed under the Agreement, whereby Transact may process Personal Data on behalf of Customer, the sub-processor list, as available through the Client Connect Portal will apply and will be incorporated herein by reference.

Annex B – Technical and Organisational Security Measures

Description of the technical and organisational measures implemented by the processor(s) / data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Measure	Description
Measures of pseudonymisation and encryption of personal data	Transact maintains formal policy and supporting procedures specific to cryptographic controls. Transact anonymizes Protected Data used in non-production and lower environments.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Transact periodically reviews the formal information security and privacy program to ensure the controls remain operational and effective in protecting the confidentiality, integrity, availability, and resiliency of data processing systems and services.
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	Transact maintains and evaluates the Continuity of Operations Plan to ensure the plan meets the Maximum Tolerable Downtime, Recovery Point Objective, and Recovery Time Objective.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing	Transact performs both internal and third-party assessments, audits, and attestation to ensure information security and privacy controls are operational and effective. This includes a SOC 2 Type II Attestation available under NDA.
Measures for user identification and authorisation	Transact ensures that access to data is authorized and authenticated based on roles, a need to know, and least privilege.
Measures for the protection of data during transmission	Transact confirms controls are operational and effective in encrypting Protected Data by implementing only non-deprecated TLS protocols while in transit.
Measures for the protection of data during storage	Transact ensures controls are operational and effective in encrypting Protected Data by implementing strong encryption while at rest.
Measures for ensuring physical security of locations at which personal data are processed	Transact relies on the physical and environmental controls provided by Public Cloud Platforms as the service provider. Leveraging the Third-Party Risk Management Program, Transact performs routine assessments of the service provider's compliance reports including the evaluation of

	said service provider's physical and environmental controls operational effectiveness.
Measures for ensuring events logging	Transact maintains logs with sufficient detail to support incident investigation, including successful and failed login attempts and changes to Protected Data.
Measures for ensuring system configuration, including default configuration	Transact maintains baseline configuration of systems including configuration policy and supporting procedures.
Measures for internal IT and IT security governance and management	Transact maintains a formal information security program with ratified policy and supporting procedures. A CISO provides oversight and governance of the Information Security Program and Transact's DPO provides oversight and governance of the Global Privacy Program
Measures for certification/assurance of processes and products	SOC 2 Type II Attestation, PCI
Measures for ensuring data minimisation	Transact employs security by design policy and principles which ensure only required data is collected.
Measures for ensuring data quality	Transact's Data Governance Committee provides policy and standards for ensuring data is accurate, relevant, complete, timely, and consistent.
Measures for ensuring limited data retention	Transact maintains data classification and handling policy with supporting procedures, a guide and retention tables.
Measures for ensuring accountability	Transact maintains a Security and Privacy Governance policy in tandem with Security Awareness Training and a Human Resources Security policy.
Measures for allowing data portability and ensuring erasure]	Transact cooperates with the Data Controller on Data Subject Access Requests.

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller (and, for transfers from a processor to a sub-processor, to the data exporter).

Measure	**Description**
Technical and organizational measures of sub-processors	Transact enters into Data Processing Agreements with its Sub-Processors including data protection obligations substantially similar to those contained in this Addendum.