

Seesaw Data Processing Agreement

(Revision November 2022)

This Data Processing Agreement and its Exhibits (“DPA”) forms part of and is subject to the terms and conditions of the Agreement (as defined below) by and between you (“Customer”) and Seesaw Learning, Inc. (“Seesaw”).

Instructions and Effectiveness

This DPA has been pre-signed on behalf of Seesaw. To enter into this DPA, Customer must:

- (a) be a customer of Seesaw;
- (b) complete the signature block below by signing and providing all relevant information; and
- (c) submit the completed and signed DPA to Seesaw at gdpr@seesaw.me.

This DPA will only be effective (as of the Effective Date) if executed and submitted to Seesaw accurately and in full accordance with this Section. Where Customer makes any deletions or other revisions to this DPA, this DPA will be null and void.

Customer signatory represents to Seesaw that he or she has the legal authority to bind Customer and is lawfully able to enter into this DPA.

This DPA will terminate automatically upon termination of the Agreement, unless earlier terminated pursuant to the terms of this DPA.

1. Definitions

"Agreement" means Seesaw’s Master Services Agreement, which govern the provision of the Services to Customer, as such terms may be updated by Seesaw from time to time. The Master Services Agreement is available at <http://web.seesaw.me/msa>.

“Customer” means a school or school district, however organized, located within the European Economic Area (EEA), Switzerland, or the United Kingdom (“UK”) that contracts with Seesaw to receive Seesaw’s Services.

"Customer Data" means any Personal Data that Seesaw processes on behalf of Customer as a Data Processor in the course of providing Services, as more particularly described in this DPA.

"Data Protection Laws" means all data protection, privacy laws, and regulations applicable to the processing of Personal Data under the Agreement, including, where applicable, EU Data Protection Law, as well as those of the European Economic Area and their member states, Switzerland, and the United Kingdom including but not limited to the United Kingdom General Data Protection Regulation, the United

Kingdom Data Protection Act 2018, and the California Consumer Privacy Act of 2018 (in each case, as amended, adopted, or superseded from time to time).

"Data Controller" means a school or school district, however organized, that contracts as a Customer with Seesaw to provide Seesaw's services to the cohort of parents, students, teachers, school officials or other end users authorized by the Customer that determines the purposes and means of the processing of Personal Data.

"Data Processor" means an entity that processes Personal Data on behalf of a Data Controller and includes "service providers" as defined under the CCPA.

"EU Data Protection Law" means (i) prior to 25 May 2018, Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of Personal Data and on the free movement of such data ("Directive") and on and after 25 May 2018, Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (General Data Protection Regulation) ("GDPR"); and (ii) Directive 2002/58/EC concerning the processing of Personal Data and the protection of privacy in the electronic communications sector and applicable national implementations of it (as may be amended, superseded or replaced).

"EEA" means, for the purposes of this DPA, the European Economic Area, United Kingdom and Switzerland.

"Personal Data" means any information relating to an identified or identifiable natural person.

"Privacy Policy" means Seesaw's Privacy Policy, which governs the provision of the Services to Customer, as such terms may be updated by Seesaw from time to time. The Privacy Policy is available at <https://web.seesaw.me/privacy-policy>.

"Processing" has the meaning given to it in the GDPR, and "process", "processes" and "processed" shall be interpreted accordingly.

"Subprocessor" means an entity that contracts with Seesaw to assist Seesaw in the Processing of Customer Data under the Agreement.

2. Relationship with the Agreement and Privacy Policy

2.1 Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Agreement, this DPA shall prevail to the extent of that conflict.

2.2 Any claims brought under or in connection with this DPA shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Agreement.

2.3 This DPA shall be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by applicable Data Protection Laws.

3. Scope and Applicability of this DPA

3.1 This DPA applies where and only to the extent that Seesaw processes Customer Data that is subject to Data Protection Laws on behalf of Customer as Data Processor in the course of providing Services pursuant to the Agreement.

4. Roles and Scope of Processing

4.1 Role of the Parties. As between Seesaw and Customer, Customer is the Data Controller of Customer Data, and Seesaw shall process Customer Data only as a Data Processor acting on behalf of Customer.

4.2. Customer Processing of Customer Data. Customer agrees and certifies that: (i) it shall comply with its obligations as a Data Controller under Data Protection Laws in respect of its processing of Customer Data and any processing instructions it issues to Seesaw; (ii) it has provided notice and obtained (or shall obtain) all consents and rights necessary under Data Protection Laws for Seesaw to process Customer Data and provide the Services pursuant to the Agreement and this DPA, or that Customer has a legitimate interest in performing a public task that permits Customer to collect Customer Data and transfer Customer Data to Seesaw to process to provide the Services to facilitate that public task; (iii) the consents it has obtained comply in all respects with Data Protection Laws.

4.3 Seesaw Processing of Customer Data. Seesaw shall process Customer Data only for the purposes described in this DPA and only in accordance with Customer's documented lawful instructions. The parties agree that this DPA and the Agreement set out the Customer's complete instructions to Seesaw in relation to the processing of Customer Data, and any processing outside the scope of these instructions (if any) shall require prior written Agreement between Customer and Seesaw, except where said processing is required under Data Protection Laws. Seesaw will, unless legally prohibited from doing so, inform Customer in writing if it reasonably believes that there is a conflict between Customer's instructions and Data Protection Laws, or otherwise seeks to process Customer Data in a manner that is inconsistent with Customer's instructions.

4.4 Details of Data Processing. (a) Subject matter: The subject matter of the data processing under this DPA is the Customer Data. (b) Purpose: The purpose of the data processing under this DPA is the provision of the Services to the Customer and the performance of Seesaw's obligations under the Agreement (including this DPA) or as otherwise agreed by the parties. (c) Nature of the processing: Seesaw provides a digital student portfolio, as described in the Agreement. (d) Categories of data subjects: Any individual accessing and/or using the Services through the Customer's account ("Users"). (e) Types of Customer Data: Account Information (such as email and name), log data, photos, videos, audio, messages, text and other data that is provided by Customer pursuant to the Agreement.

5. Subprocessing

5.1 Authorized Subprocessors. Customer agrees that Seesaw may engage Subprocessors to process Customer Data on Customer's behalf. The Subprocessors currently engaged by Seesaw and authorized by Customer are listed at: <https://web.seesaw.me/subprocessor>.

5.2 Subprocessor Obligations. Seesaw shall: (i) enter into a written agreement with the Subprocessor imposing data protection terms that require the Subprocessor to protect the Customer Data to the standard required by Data Protection Laws; and (ii) remain responsible for its compliance with the

obligations of this DPA and for any acts or omissions of the Subprocessor that cause Seesaw to breach any of its obligations under this DPA.

5.3 Authorization of Subprocessors. Customer agrees that by agreeing to this DPA it has reviewed all of the Subprocessors utilized by Seesaw in the processing of Customer Data and expressly authorizes Seesaw to utilize those Subprocessors.

5.4 Changes to Subprocessors. When any new Subprocessor is engaged, Seesaw will update its list of current subprocessors here: <https://web.seesaw.me/subprocessor>. To receive notice of updates to the list of subprocessors please subscribe at the link provided above. Customer may object in writing to Seesaw's appointment of a new Subprocessor within five (5) calendar days of such notice, provided that such objection is based on reasonable grounds relating to data protection. In such event, the parties shall discuss such concerns in good faith with a view to achieving resolution. If this is not possible, Customer may suspend or terminate the Agreement and request a pro-rated refund of any fees paid.

6. Security

6.1 Security Measures. Seesaw shall implement and maintain appropriate technical and organizational security measures to protect Customer Data from Security Incidents and to preserve the security and confidentiality of the Customer Data, in accordance with Seesaw's security standards described in <https://help.seesaw.me/hc/en-us/articles/203258429> and as described in **Exhibit B**.

6.2 Updates to Security Measures. Customer is responsible for reviewing the information made available by Seesaw relating to data security and making an independent determination as to whether the Services meet Customer's requirements and legal obligations under Data Protection Laws. Customer acknowledges that the Security Measures are subject to technical progress and development and that Seesaw may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services purchased by the Customer.

6.3 Audits of Compliance. Where Data Protection Laws afford Customer an audit right, and no more than once per year (except where legally required), Seesaw will allow Customer or a third-party auditor appointed by Customer to conduct audits (including inspections) to verify Seesaw's compliance with its obligations under this Data Processing Agreement.

6.4 Additional Business Terms for Audits.

(a) Following receipt by Seesaw of an audit request, Seesaw and Customer will discuss and agree in advance on the reasonable start date, scope and duration of, and security and confidentiality controls applicable to, any audit. Any audit must be: (i) conducted during Seesaw's regular business hours; (ii) with reasonable advance notice to Seesaw; (iii) carried out in a manner that prevents unnecessary disruption to Seesaw's operations; and (iv) subject to reasonable confidentiality procedures.

(b) Seesaw may charge a fee (based on Seesaw's reasonable costs) for any audit. Seesaw will provide Customer with further details of any applicable fee, and the basis of its calculation, in advance of any such audit. Customer will be responsible for any fees charged by any third-party auditor appointed by Customer to execute any such audit.

(c) Seesaw may object to any third-party auditor appointed by Customer to conduct any audit under Section 7 if the auditor is, in Seesaw's reasonable opinion, not suitably qualified or independent, a

competitor of Seesaw, or otherwise manifestly unsuitable. Any such objection by Seesaw will require Customer to appoint another auditor or conduct the audit itself.

(d) Nothing in these Data Processing Terms will require Seesaw either to disclose to Customer or its third-party auditor, or to allow Customer or its third-party auditor to access:

- (i) any data of any other customer of Seesaw;
- (ii) any Seesaw Entity's internal accounting or financial information;
- (iii) any trade secret of a Seesaw Entity;
- (iv) any information that, in Seesaw's reasonable opinion, could: (A) compromise the security of Seesaw's systems or premises; or (B) cause Seesaw to breach its obligations under the Data Protection Legislation or its security and/or privacy obligations to Customer or any third party; or
- (v) any information that Customer or its third-party auditor seeks to access for any reason other than the good faith fulfilment of Customer's obligations under the Data Protection Legislation.

7. International Transfers

1. Cross-Border Transfers of Customer Data. Customer authorizes Seesaw and its Subprocessors to transfer Customer Data across international borders, including from the European Economic Area, Switzerland, and/or the United Kingdom to the United States.
2. Seesaw Data Transfer Impact Assessment Questionnaire. Seesaw agrees that it has provided true, complete, and accurate responses to the Data Transfer Impact Assessment Questionnaire attached hereto as **Exhibit A**.
3. EEA Controller to Processor Standard Contractual Clauses. If Customer Data originating in the European Economic Area is transferred by Customer to Seesaw in a country that has not been found to provide an adequate level of protection under applicable Data Protection Laws, the parties agree that the transfer shall be governed by the Controller to Processor Standard Contractual Clauses (**Module Two**) attached hereto as **Exhibit C**. The parties agree that: (i) the certification of deletion required by Clause 8.5 and Clause 16(d) of the Controller to Processor Standard Contractual Clauses will be provided upon Customer's written request; (ii) the measures Seesaw is required to take under Clause 8.6(c) of the Controller to Processor Standard Contractual Clauses will only cover Seesaw's impacted systems; (iii) Seesaw may engage Subprocessors using European Commission Decision C(2010)593 Standard Contractual Clauses for Controllers to Processors or any other adequacy mechanism provided that such adequacy mechanism complies with applicable Data Protection Laws and such use of Subprocessors shall not be considered a breach of Clause 9 of the Controller to Processor Standard Contractual Clauses; (iv) the termination right contemplated by Clause 14(f) and Clause 16(c) of the Controller to Processor Standard Contractual Clauses will be limited to the termination of the Controller to Processor Standard Contractual Clauses, in which case, the corresponding Processing of Customer Data affected by such termination shall be discontinued unless otherwise agreed by the parties; (v) unless otherwise stated by Seesaw, Customer will be responsible for communicating with data subjects pursuant to Clause 15.1(a) of the Controller to Processor Standard Contractual Clauses; (vi) the information required under Clause 15.1(c) will be provided upon Customer's written request; (vii) notwithstanding anything to the contrary, Customer will reimburse Seesaw for all costs and expenses incurred by Seesaw in connection with the performance of Seesaw's obligations under Clause 15.1(b) and Clause 15.2 of the Controller to

Processor Standard Contractual Clauses without regard for any limitation of liability set forth in the Agreement; and (vii) the audit described in Clause 8.9 of the Standard Contractual Clauses shall be carried out in accordance with Section 6 of this DPA. Each party's signature to this DPA shall be considered a signature to the Standard Contractual Clauses to the extent that the Standard Contractual Clauses apply hereunder.

4. Customer Data Transfer Impact Assessment Questionnaire. Customer agrees that it has provided true, complete, and accurate responses to the Customer Data Transfer Impact Assessment Questionnaire attached hereto as **Exhibit D**.
5. EEA Processor to Controller Standard Contractual Clauses. If Customer Data originating in the European Economic Area is transferred by Seesaw to Customer in a country that has not been found to provide an adequate level of protection under applicable Data Protection Laws, the parties agree that the transfer shall be governed by the Processor to Controller Standard Contractual Clauses (**Module Four**), attached hereto as **Exhibit E**. The parties agree that: (i) the information required by Clause 8.1(d) of the Processor to Controller Standard Contractual Clauses will be provided upon Customer's written request, and (ii) the audit described in Clause 8.3(b) of the Processor to Controller Standard Contractual Clauses shall be carried out in accordance with Section 6 of this DPA. Each party's signature to this DPA shall be considered a signature to the Processor to Controller Standard Contractual Clauses to the extent that the Processor to Controller Standard Contractual Clauses apply hereunder.
6. Data Exports from the United Kingdom under the Standard Contractual Clauses. For data transfers governed by UK Data Protection Laws and Regulations, the Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as revised under Section 18 of those Mandatory Clauses ("Approved Addendum") shall apply (Annex III).
7. Data Exports from Switzerland under the Standard Contractual Clauses. For data transfers governed by Swiss Data Protection Laws, the Standard Contractual Clauses also apply to the transfer of information relating to an identified or identifiable legal entity where such information is protected similarly as Personal Data under Swiss Data Protection Laws until such laws are amended to no longer apply to a legal entity.
8. Data Transfer Impact Assessment Outcome. Taking into account the information and obligations set forth in this DPA and, as may be the case for a party, such party's independent research, to the parties' knowledge, the Company Personal Data originating in the European Economic Area, Switzerland, and/or the United Kingdom that is transferred pursuant to the attached Standard Contractual Clauses to a country that has not been found to provide an adequate level of protection under applicable Data Protection Laws is afforded a level of protection that is essentially equivalent to that guaranteed by applicable Data Protection Laws.

8. Additional Security

8.1 Confidentiality of Processing. Seesaw shall ensure that any person who is authorized by Seesaw to process Customer Data (including its staff, agents and subcontractors) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).

8.2 Security Incident Response. Upon becoming aware of a Security Incident, Seesaw shall notify Customer without undue delay and shall provide timely information relating to the Security Incident as it becomes known or as is reasonably requested by Customer.

9. Return or Deletion of Data

9.1 Upon termination or expiration of the Agreement, Seesaw shall (at Customer's election) delete or return to Customer all Customer Data (including copies) in its possession or control, unless a student or parent has created an independent account with Seesaw and wishes to retain their own information. This requirement shall not apply to the extent Seesaw is required by applicable law to retain some or all of the Customer Data.

10. Cooperation

10.1 The Services provide Customer with a number of controls that Customer may use to retrieve, correct, delete or restrict Customer Data, which Customer may use to assist it in connection with its obligations under the GDPR or other applicable Data Protection Laws, including its obligations relating to responding to requests from data subjects, report data breaches, if any, to the data subject and data protection authorities, undertake a data protection impact analysis including consulting with the relevant data protection authorities for any new, high risk processing, or respond to requests from applicable data protection authorities. To the extent that Customer is unable to independently access the relevant Customer Data within the Services, Seesaw shall provide reasonable cooperation to assist Customer to respond to any requests from individuals or applicable data protection authorities relating to the processing of Customer Data under the Agreement. In the event that any such request is made directly to Seesaw, Seesaw shall not respond to such communication directly without Customer's prior authorization, unless legally compelled to do so. If Seesaw is required to respond to such a request, Seesaw shall promptly notify Customer and provide it with a copy of the request unless legally prohibited from doing so. It is Customer's responsibility to verify the identity of a data subject making such a request before Seesaw will respond to any request.

11. Termination

11.1 Customer may terminate this agreement by providing 30 days written notice at any time. No fees previously paid by Customer will be refunded.

11.2 Customer may terminate this agreement for a material breach that is not corrected by Seesaw within 30 days and request a pro-rated refund of any fees paid.

12. Miscellaneous

Seesaw's Data Protection Officer is Megan Bradley, and she can be reached at gdpr@seesaw.me. Seesaw's data protection supervisory authority is Ireland. VeraSafe has been appointed as Seesaw's representative in the European Union and the United Kingdom for data protection matters. VeraSafe can be contacted at: <https://www.verasafe.com/privacy-services/contact-article-27-representative>. Alternatively, VeraSafe can be contacted at Unit 3D North Point House, North Point Business Park, New Mallow Road, Cork T23AT2P, Ireland. Their phone number is +1 617-398-7067. For inquiries specific to the United Kingdom VeraSafe can be contacted at VeraSafe United Kingdom Ltd., 37 Albert

Embankment, London SE1 7TL, United Kingdom at: <https://verasafe.com/public-resources/contact-data-protection-representative>. Their phone number is +44 (20) 4532 2003.

List of Exhibits

- Exhibit A: SEESAW DATA TRANSFER IMPACT ASSESSMENT QUESTIONNAIRE
- Exhibit B: TECHNICAL AND ORGANIZATIONAL MEASURES
- Exhibit C (Annex I, II, III): CONTROLLER TO PROCESSOR STANDARD CONTRACTUAL CLAUSES
- Exhibit D: CUSTOMER DATA TRANSFER IMPACT ASSESSMENT QUESTIONNAIRE
- Exhibit E (Annex I, II): PROCESSOR TO CONTROLLER STANDARD CONTRACTUAL CLAUSES

The parties' authorized signatories have duly executed this DPA:

Customer Name: _____

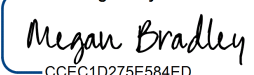
Signature: _____

Name: _____

Title: _____

Date: _____

Email: _____

DocuSigned by:

CCEC1D275E584ED
 Megan Bradley
 Counsel, Seesaw Learning Inc.

11/8/2022

 Date

EXHIBIT A TO THE DATA PROCESSING AGREEMENT
SEESAW DATA TRANSFER IMPACT ASSESSMENT QUESTIONNAIRE

This Exhibit A forms part of the DPA. Capitalized terms not defined in this Exhibit A have the meaning set forth in the DPA.

1. What countries will Customer Data that is transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom be stored in or accessed from? If this varies by region, please specify each country for each region.
 - a. **Answer:** Customer Data will be stored in the United States.
2. What are the categories of data subjects whose Customer Data will be transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom?
 - a. **Answer:** Students, Family Member, Teachers, Administrators, and other school officials as contemplated by the Agreement.
3. What are the categories of Customer Data transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom?
 - a. **Answer:** User Account Information (such as email and name), log data, Journal Content such as photos, videos, audio, messages, text, and other data that is provided by Customer.
4. Will any Customer Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences be transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom? If so, are there any restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures?
 - a. **Answer:** User-generated content may include data concerning health and may be inadvertently transferred to Seesaw. Seesaw expressly requests that the Customer not transfer any Customer Data that is health data to Seesaw. Seesaw does not seek and will not store in a structured manner any Customer Data that is health data. Seesaw also collects and processes information from children for the limited purposes in the Agreement.
5. What is the frequency of the transfer of Customer Data outside of outside of the European Economic Area, Switzerland, and/or the United Kingdom? E.g., is Customer Data transferred on a one-off or continuous basis?
 - a. **Answer:** Customer Data is transferred on a continuous basis to servers located in the United States when the Services are used.

6. Broadly speaking, what are the services to be provided and the corresponding purposes for which Customer Data is transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom?
 - a. **Answer:** Seesaw provides a digital student portfolio, as described in the Agreement. The purpose of the data processing under this DPA is the provision of the Services to the Customer and the performance of Seesaw's obligations under the Agreement (including this DPA) or as otherwise agreed by the parties. For example, Customer Data will be used to provide the Seesaw Service and answer technical support questions.

7. What is the period for which the Customer Data will be retained, or, if that is not possible, the criteria used to determine that period?
 - a. **Answer:** For the duration of the Agreement and as needed thereafter for Seesaw's compliance purposes, as described in the DPA.

8. What business sector is Seesaw involved in?
 - a. **Answer:** Education technology.

9. When Customer Data is transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom to Seesaw, how is it transmitted to Seesaw? Is the Customer Data in plain text, pseudonymized, and/or encrypted?
 - a. **Answer:** Seesaw uses TLS 1.3 security at the network level to ensure all account information and journal content is transmitted securely.

10. Please list the Subprocessors that will have access to Customer Data that is transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom:
 - a. **Answer:** As set forth at the following URL: <https://web.seesaw.me/subprocessor>.

11. Is Seesaw subject to any laws in a country outside of the European Economic Area, Switzerland, and/or the United Kingdom where Customer Data is stored or accessed from that would interfere with Seesaw fulfilling its obligations under the attached Standard Contractual Clauses? For example, FISA Section 702 or U.S. Executive Order 12333. If yes, please list these laws.
 - a. **Answer:** Seesaw is subject to laws in the United States. As of the effective date of the DPA, no court has found Seesaw to be eligible to receive process issued under the laws contemplated by Question 11, including FISA Section 702, and no such court action is pending.

12. Has Seesaw ever received a request from public authorities for information pursuant to the laws contemplated by Question 11 above (if any)? If yes, please explain.
 - a. **Answer:** As of the effective date of the DPA, Seesaw has not received any national security orders of the type described in Paragraphs 150-202 of the judgment in the CJEU Case C-311/18, Data Protection Commissioner v Facebook Ireland Limited and Maximilian Schrems, nor is Seesaw aware of any such orders in progress.

13. Has Seesaw ever received a request from public authorities for Personal Data of individuals located in the European Economic Area, Switzerland, and/or the United Kingdom? If yes, please explain.

a. **Answer:** No.

14. What safeguards will Seesaw apply during transmission and to the processing of Customer Data in countries outside of the European Economic Area, Switzerland, and/or the United Kingdom that have not been found to provide an adequate level of protection under applicable Data Protection Laws?

a. **Answer:** As set forth in **Exhibit B**.

EXHIBIT B TO THE DATA PROCESSING AGREEMENT: TECHNICAL AND ORGANIZATIONAL MEASURES

This Exhibit B forms part of the DPA. Capitalized terms not defined in this Exhibit B have the meaning set forth in the DPA.

Seesaw shall implement and maintain appropriate technical and organisational measures designed to protect Customer Data. At a minimum, such measures will include:

- Seesaw uses TLS 1.3 security at the network level to ensure account information and journal content is transmitted securely. Seesaw requires TLS 1.2 at a minimum; TLS 1.0 and 1.1 are not supported.
- Personally identifiable information (PII), like names, email addresses, phone numbers, messages, journal content, stored in Seesaw is encrypted at rest.
- Multi-Factor Authentication provides an extra layer of sign-in security. MFA helps keep out anyone who shouldn't have access to your account by requiring a verification code (sent via email) in addition to your password before your account can be accessed.
- Passwords are salted and hashed using PBKDF2.
- Seesaw routinely conducts 3rd party security audits to verify the security and integrity of our systems and internal controls.
- The Seesaw application is penetration and security tested by an independent third party annually.
- Password requirements for new accounts and password resets follow the guidelines of the Cybersecurity Infrastructure and Security Agency.
- Data is stored in access-controlled data centers operated by industry leading partners with years of experience in large-scale data centers with 24/7 monitoring.
- User information is stored redundantly and backed up in geographically distributed data centers. We utilize multiple distributed servers to ensure high levels of uptime and to ensure that we can restore availability and access to personal data in a timely manner.
- We have adopted an internal data access policy that restricts access to personally identifiable information to a limited number of employees with a specific business need (such as for technical support).
- Employees undergo a background check before beginning employment at Seesaw, sign a nondisclosure agreement, and immediately lose access to all internal systems and data when terminated.
- We routinely monitor our systems for security breaches and attempts at inappropriate access.
- We use encrypted QR codes for family and student access to journal content.

EXHIBIT C TO THE DATA PROCESSING AGREEMENT
CONTROLLER TO PROCESSOR STANDARD CONTRACTUAL CLAUSES

This Exhibit C forms part of the DPA.

SECTION I

Clause 1

Purpose and scope

- (a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) for the transfer of personal data to a third country.
- (b) The Parties:
 - (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and
 - (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')have agreed to these standard contractual clauses (hereinafter: 'Clauses').
- (c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
- (d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.
- (e) To the extent applicable hereunder, these Clauses also apply mutatis mutandis to the Parties processing of personal data that is subject to the Swiss Federal Act on Data Protection. Where applicable, references to EU Member State law or EU supervisory authorities shall be modified to include the appropriate reference under Swiss law as it relates to transfers of personal data that are subject to the Swiss Federal Act on Data Protection.
- (f) To the extent applicable hereunder, these Clauses, as supplemented by Annex III, also apply mutatis mutandis to the Parties' processing of personal data that is subject to UK Data Protection Laws (as defined in Annex III).

Clause 2

Effect and invariability of the Clauses

- (a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to

add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

- (b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

- (a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
 - (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
 - (ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);
 - (iii) Clause 9(a), (c), (d) and (e);
 - (iv) Clause 12(a), (d) and (f);
 - (v) Clause 13;
 - (vi) Clause 15.1(c), (d) and (e);
 - (vii) Clause 16(e);
 - (viii) Clause 18(a) and (b).
- (b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

- (a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
- (b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
- (c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Optional

Docking clause – Omitted

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

MODULE TWO: Transfer controller to processor

8.1 Instructions

- (a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
- (b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I. B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

- (a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
- (b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- (c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is

not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

- (d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

- (i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- (ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
- (iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- (iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

- (a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
- (b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.
- (c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In

deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

- (d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
- (e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

- (a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least five (5) calendar days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.
- (b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
- (c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
- (d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.
- (e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

MODULE TWO: Transfer controller to processor

- (a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.
- (b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
- (c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

- (a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

MODULE TWO: Transfer controller to processor

- (b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
- (c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
 - (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
 - (ii) refer the dispute to the competent courts within the meaning of Clause 18.
- (d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
- (e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
- (f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

MODULE TWO: Transfer controller to processor

- (a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
- (b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.
- (c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.
- (d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
- (e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
- (f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.
- (g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

MODULE TWO: Transfer controller to processor

- (a) Where the data exporter is established in an EU Member State, the following section applies: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679, the following section applies: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679, the following section applies: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

- (b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

MODULE TWO: Transfer controller to processor

- (a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
- (b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
 - (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
 - (ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;
 - (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

- (c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
- (d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
- (e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).
- (f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

MODULE TWO: Transfer controller to processor

15.1 Notification

- (a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
 - (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
 - (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
- (b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as

possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

- (c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).
- (d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
- (e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

- (a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).
- (b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.
- (c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

- (a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
- (b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data

importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

- (c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
 - (i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
 - (ii) the data importer is in substantial or persistent breach of these Clauses; or
 - (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

- (d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.
- (e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

MODULE TWO: Transfer controller to processor

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

- (a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- (b) The Parties agree that those shall be the courts of Ireland.
- (c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
- (d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

ANNEX I

A. LIST OF PARTIES

MODULE TWO: Transfer controller to processor

Data exporter(s):

1. Name: Customer.
2. Address: As described in the DPA.
3. Contact person's name, position, and contact details: the Customer contact described in the DPA.
4. Activities relevant to the data transferred under these Clauses: As set forth in Exhibit A.
5. Role (controller/processor): Controller.

Data importer(s):

1. Name: Seesaw Learning, Inc.
2. Address: 548 Market Street, PMB 98963, San Francisco, CA 94104 USA
3. Contact person's name, position, and contact details: Megan Bradley, Counsel, Tel. +1 415-870-4468; e-mail: gdpr@seesaw.me
4. Activities relevant to the data transferred under these Clauses: As set forth in Exhibit A.
5. Role (controller/processor): Processor.

.....

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

Categories of data subjects whose personal data is transferred

.....As described in Exhibit A.....

Categories of personal data transferred

.....As described in Exhibit A.....

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

.....As described in Exhibit A.....

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

.....As described in Exhibit A.....

Nature of the processing

.....As described in Exhibit A.....

Purpose(s) of the data transfer and further processing

.....As described in Exhibit A.....

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

.....As described in Exhibit A.....

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

.....As described in Exhibit A.....

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer controller to processor

.....The supervisory authority mandated by Clause 13. If no supervisory authority is mandated by Clause 13, then the Irish Data Protection Commission (DPC), and if this is not possible, then as otherwise agreed by the parties consistent with the conditions set forth in Clause 13.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE TWO: Transfer controller to processor

Description of the technical and organisational measures implemented by the 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.

Seesaw shall implement and maintain appropriate technical and organisational measures designed to protect personal data in accordance with **Exhibit B**.

Pursuant to Clause 10(b), Seesaw will provide Customer assistance with data subject requests in accordance with the DPA.

ANNEX III

Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

PART I

Table 1: Parties

The information required for Table 1 of Part One of the Approved Addendum is set out in Exhibit C, Annex I of this DPA.

Table 2: Selected SCCs, Modules and Selected Clauses

The information required for Table 2 of Part One of the Approved Addendum is set out in Exhibit C and E of this DPA (as applicable).

Table 3: Appendix Information

The information required for Table 3 of Part One of the Approved Addendum is set out in Exhibit D and Exhibit C, Annex I of this DPA (as applicable).

Table 4: Ending this Addendum when the Approved Addendum Changes

For the purposes of Table 4 of Part One of the Approved Addendum, neither party may end the Approved Addendum when it changes.

PART II

Mandatory Clauses of the Approved Addendum, being the template [Addendum B.1.0](#) issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

EXHIBIT D TO THE DATA PROCESSING AGREEMENT

CUSTOMER DATA TRANSFER IMPACT ASSESSMENT QUESTIONNAIRE

This Exhibit D forms part of the DPA. Capitalized terms not defined in this Exhibit D have the meaning set forth in the DPA.

Throughout the term of the Agreement, Customer will promptly notify Seesaw's Designated POC within ten (10) business days if there are material changes to the responses set forth in this Exhibit C following the effective date of the Agreement and work with Seesaw to update Customer's responses set forth in this Customer Data Transfer Impact Assessment Questionnaire.

1. What countries will Customer Data that is transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom be stored in or accessed from by Customer? If this varies by region, please specify each country for each region.
 - a. **Answer:** Those countries where Customer conducts its business activities which may include, but are not limited to, the United States.
2. What are the categories of data subjects whose Customer Data will be transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom?
 - a. **Answer:** Data subjects whose Customer Data will be provided by Seesaw pursuant to the Processor to Controller Standard Contractual Clauses which may include, but are not limited to, those data subjects contemplated by Seesaw's response to Question 2, Exhibit A.
3. What are the categories of Customer Data transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom?
 - a. **Answer:** Customer Data that will be provided by Seesaw pursuant to the Processor to Controller Standard Contractual Clauses which may include, but is not limited to, the Customer Data contemplated by Seesaw's response to Question 3, Exhibit A.
4. Will any Customer Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences be transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom? If so, are there any restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures?
 - a. **Answer:** No.
5. What is the nature and purpose for which Customer Data is transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom by Seesaw to Customer?

- a. **Answer:** Customer Data is transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom so that Customer can operate its business.
6. What is the frequency of the transfer of Customer Data outside of the European Economic Area, Switzerland, and/or the United Kingdom? E.g., is Customer Data transferred on a one-off or continuous basis?
 - a. **Answer:** Customer Data is transferred by Seesaw to Customer in accordance with the standard functionality of the Services or as otherwise agreed upon by the parties.
7. When Customer Data is transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom to Customer, how is it transmitted to Customer? Is the Customer Data in plain text, pseudonymized, and/or encrypted?
 - a. **Answer:** Customer Data is transferred and made available to Customer directly through the Services, accessible only to Customer's authorized users.
8. What is the period for which the Customer Data will be retained, or, if that is not possible, the criteria used to determine that period?
 - a. **Answer:** Customer will retain Customer Data in accordance with the applicable Customer privacy notice or policy that governs such Customer Data.
9. Please list the Customer subprocessors that will have access to Customer Data that is transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom.
 - a. **Answer:** Those subprocessors involved in the operation of Customer's business.
10. Is Customer subject to any laws in a country outside of the European Economic Area, Switzerland, and/or the United Kingdom where Customer Data is stored or accessed from that would interfere with Customer fulfilling its obligations under the Processor to Controller Standard Contractual Clauses? For example, FISA Section 702. If yes, please list these laws.
 - a. **Answer:** As of the effective date of the Agreement, no court has found Customer to be eligible to receive process issued under the laws contemplated by Question 10, including FISA Section 702 and no such court action is pending.
11. Has Customer ever received a request from public authorities for information pursuant to the laws contemplated by Question 10 above (if any)? If yes, please explain.
 - a. **Answer:** No.
12. Has Customer ever received a request from public authorities for Personal Data of individuals located in European Economic Area, Switzerland, and/or the United Kingdom? If yes, please explain.
 - a. **Answer:** No.

EXHIBIT E TO THE DATA PROCESSING AGREEMENT
PROCESSOR TO CONTROLLER STANDARD CONTRACTUAL CLAUSES

This Exhibit E forms part of the DPA.

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

(e) To the extent applicable hereunder, these Clauses also apply mutatis mutandis to the Parties processing of personal data that is subject to the Swiss Federal Act on Data Protection. Where applicable, references to EU Member State law or EU supervisory authorities shall be modified to include the appropriate reference under Swiss law as it relates to transfers of personal data that are subject to the Swiss Federal Act on Data Protection.

(f) To the extent applicable hereunder, these Clauses, as supplemented by Annex II, also apply mutatis mutandis to the Parties' processing of personal data that is subject to UK Data Protection Laws (as defined in Annex II).

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

- (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
- (ii) Clause 8.1 (b) and Clause 8.3(b);
- (v) Clause 13;
- (vi) Clause 15.1(c), (d) and (e);
- (vii) Clause 16(e);
- (viii) Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Optional

Docking clause – Omitted

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

MODULE FOUR: Transfer processor to controller

8.1 Instructions

- (a) The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.
- (b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.
- (c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.
- (d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

8.2 Security of processing

- (a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.
- (b) The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.
- (c) The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.3 Documentation and compliance

- (a) The Parties shall be able to demonstrate compliance with these Clauses.
- (b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

Clause 9

Use of sub-processors – Omitted

Clause 10

Data subject rights

MODULE FOUR: Transfer processor to controller

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

Clause 12

Liability

MODULE FOUR: Transfer processor to controller

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

Clause 13

Supervision – Omitted

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

MODULE FOUR: Transfer processor to controller *(this clause is only applicable where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)*

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination— including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

MODULE FOUR: Transfer processor to controller (*this clause is only applicable where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU*)

15.1 Notification

- (a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
- (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
 - (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
- (b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
- (c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).
- (d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
- (e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

- (a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

MODULE FOUR: Transfer processor to controller

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

Choice of forum and jurisdiction

MODULE FOUR: Transfer processor to controller

Any dispute arising from these Clauses shall be resolved by the courts of Ireland.

ANNEX I

A. LIST OF PARTIES

MODULE FOUR: Transfer processor to controller

1. Data exporter(s):

- 1. Name: Seesaw Learning, Inc.
- 2. Address: 548 Market Street, PMB 98963, San Francisco, CA 94104 USA
- 3. Contact person’s name, position and contact details: Megan Bradley, Counsel, Tel. +1 415-870-4468; e-mail: gdpr@seesaw.me
- 4. Activities relevant to the data transferred under these Clauses: As set forth in Exhibit A.
- 5. Role (controller/processor): Processor.

2. Data importer(s):

- 1. Name: Customer.
- 2. Address: As described in the DPA.
- 3. Contact person’s name, position and contact details: the Customer contact described in the DPA.
- 4. Activities relevant to the data transferred under these Clauses: As set forth in Exhibit A.
- 5. Role (controller/processor): Controller.

B. DESCRIPTION OF TRANSFER

MODULE FOUR: Transfer processor to controller

Categories of data subjects whose personal data is transferred

.....As described in Exhibit D.....

Categories of personal data transferred

.....As described in Exhibit D.....

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

.....As described in Exhibit D.....

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

.....As described in Exhibit D.....

Nature of the processing

.....As described in Exhibit D.....

Purpose(s) of the data transfer and further processing

.....As described in Exhibit D.....

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

.....As described in Exhibit D.....

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

.....As described in Exhibit D.....

ANNEX II

Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018

UK Addendum to the EU Commission Standard Contractual Clauses

The terms of Exhibit C, Annex III also apply to this Exhibit E.