

Respondus Data Processing Agreement

Effective Aug. 27, 2020

This Data Processing Agreement (“DPA”) is incorporated by reference into the subscription license agreement (the “License Agreement”) between Respondus, Inc. (“Respondus”) and Licensee (as defined below) for Licensee’s access to and use of Respondus Service(s) (as defined below) and related technical support to Licensee as if completely set forth therein. This DPA reflects the parties’ agreement with respect to the processing and security of Personal Data (also referred to as Personal Information in the License Agreement) from or about Licensee’s students (“Students”) under the License Agreement (“Licensee Data”).

Definitions

Unless otherwise defined herein, capitalized terms and expressions used in this Agreement shall have the following meaning:

“Agreement” means this Data Processing Agreement and all Annexes.

“Applicable Data Protection Law” means

- (i) GDPR and any applicable national data protection laws, as may be amended or superseded from time to time;
- (ii) All applicable law about the processing of personal data and privacy.

“Controller,” “Processor,” “Data Subject,” “Personal Data,” and **“Processing”** shall have the meanings given in Applicable Data Protection Law.

“Documentation” means the License Agreement, Terms of Use, End User License Agreements, and the User Guide for each Service as provided by Respondus to each Licensee and found at the Respondus website, <https://respondus.com/>

“GDPR” means Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

“Licensee” means the Customer institution that is purchasing a license to operate the Respondus Service.

“Licensee Data” means data, including Personal Data, for which the Licensee is the Controller.

“Privacy Shield” means the EU-US Privacy Shield self-certification program operated by the U.S. Department of Commerce and approved by the European Commission pursuant to Decision C (2016)4176 of July 12, 2016.

“Security Incident” means a breach of Respondus’ security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Licensee Data.

“Service” or **“Respondus Service”** means the services provided pursuant to a subscription to one or more of the following Respondus products: LockDown Browser and Respondus Monitor. A further description of each Service can be found in the Documentation.

“Standard Contractual Clauses” means Annex 1, attached to and forming part of this DPA pursuant to the European Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC.

“Sub-Processor” means any third-party Processors engaged directly by Respondus to assist with Respondus’ processing of Licensee Data.

“Supervisory Authority” means an independent public authority which is established by an EU Member State pursuant to the GDPR.

Data Processing

Relationship of the Parties

The parties acknowledge and agree that under the License Agreement, Licensee is the Controller and Respondus is a Processor, appointed to process the Licensee Data on the Licensee’s behalf. Each party shall comply with the obligations that apply to it under Applicable Data Protection Law.

Purpose

Licensee uses the Services to monitor certain activities of its Students, and in doing so it gathers the Licensee Data regarding its Students. The parties acknowledge that Licensee Data contains Personal Data under the Applicable Data Protection Law. Respondus stores and processes some of the Licensee Data on its servers as part of the Services. The Licensee maintains and controls all access to the Licensee Data in its account, and Respondus has access only by virtue of maintaining the servers and providing the software for the Services. The nature of the processing and the type of data processed is described in the Documentation and the duration of the processing is the term specified in the Documentation. Respondus agrees that it will not access any Licensee Data except (i) as necessary for the operation of the Services, as described in the Documentation and (ii) as expressly permitted by the Licensee (together, the “Permitted Purpose”), except where otherwise required by any law applicable to the Licensee.

Customer Instructions

The parties agree that this DPA and the Documentation constitute Licensee’s documented instructions regarding Respondus’ processing of Licensee Data (“Documented Instructions”). Respondus shall Process Licensee Data on behalf of and only in accordance with Documented Instructions for the following purposes: (i) Processing in accordance with the Documentation; (ii) Processing initiated by Users in their use of the Services; and (iii) Processing to comply with other documented reasonable

instructions provided by Licensee (e.g., via email) where such instructions are consistent with the terms of the Agreement.

Confidentiality of Licensee Data

Respondus shall treat Licensee Data as Confidential Information. Respondus will not access or use, or disclose to any third party, any Customer Data, except, in each case, as necessary to maintain or provide the Services, or as necessary to comply with the law or a valid and binding order of a governmental body (such as a subpoena or court order). If compelled to disclose Licensee Data to a governmental body, then Respondus will give Licensee reasonable notice of the demand to allow Licensee to seek a protective order or other appropriate remedy unless Respondus is legally prohibited from doing so. If the Standard Contractual Clauses apply, nothing in this section varies or modifies the Standard Contractual Clauses.

Confidentiality of Respondus Personnel

Respondus will ensure that its personnel engaged in the processing of Licensee Data (i) will process such data only on Documented Instructions from Licensee or as described in this DPA, and (ii) will be obligated to maintain the confidentiality and security of such data. Respondus shall impose appropriate obligations upon its personnel, including relevant obligations regarding confidentiality, data protection and data security. Respondus shall provide periodic data privacy and security training and awareness to its employees with access to Licensee Data, in accordance with applicable Data Protection Requirements and industry standards.

Security

Respondus shall implement and maintain appropriate technical and organizational measures to protect the Licensee Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. Such measures shall have regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the nature, likelihood and severity of the risk to the rights and freedoms of natural persons. Such measures shall include, as appropriate:

- a) the pseudonymization or encryption of personal data;
- b) ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
- d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

Data Encryption

Licensee Data (including any Personal Data therein) in transit over public networks between Licensee and Respondus, or between Respondus data centers, is encrypted.

Respondus also encrypts Licensee Data stored at rest in its hosting servers.

Sub-Processing

Licensee acknowledges that Respondus' servers that host the Services are controlled and operated by a third-party hosting provider and that such provider is a Sub-Processor under the Applicable Data

Protection Law. Licensee hereby consents to Respondus appointing Amazon Web Services (“AWS”) as such a Sub-Processor. Respondus may change or appoint additional Sub-Processors by posting notice (including the identity and details of the processing to be performed) at the following URL: web.respondus.com/privacy/subprocessors/. Respondus shall impose data protection terms on any Sub-Processor that are consistent with the terms of this DPA and the Applicable Data Protection Laws. If Licensee declines to consent to Respondus’ appointment of a Sub-Processor, Licensee may elect to suspend or terminate the License Agreement and this DPA, subject to payment of all fees due for services rendered.

Data Transfers

Licensee acknowledges that Respondus' servers are located outside of the European Economic Area ("EEA") and that the Licensee Data will be transferred outside of the EEA as part of the Services. Licensee is responsible to establish the legal basis for such transfer. To facilitate the transfer, the parties shall take such measures as are necessary to ensure the transfer is in compliance with Applicable Data Protection Law. Such measures may include (without limitation) transferring the Licensee Data to a recipient in the United States that has certified its compliance with the EU-US Privacy Shield, or to a recipient that has executed standard contractual clauses adopted or approved by the European Commission.

Cooperation and Data Subjects’ Rights

Assistance

During the Term, Respondus shall provide reasonable assistance to Licensee to respond to (a) a request from a Data Subject to exercise any of its rights under Applicable Data Protection Law (including its rights of access, correction, objection, erasure and data portability, as applicable); and (b) any other correspondence, inquiry or complaint received from a Data Subject, regulator or third party in connection with the processing of the Licensee Data as required under Applicable Data Protection Law.

Respondus shall notify the Licensee immediately if it considers that any of the Licensee's instructions infringe the Applicable Data Protection Law.

Direct Requests

Should a Data Subject contact Respondus with regard to access, correction or deletion of its personal data (or any other rights under Applicable Data Protection Law), Respondus shall promptly inform the Licensee, and in any case no later than two (2) business days after receipt of any Data Subject requests which identify the Licensee to be contacted, by sending a written notice and attaching a copy of the request sent by the Data Subject; the Licensee authorizes Respondus to inform the Data Subject that Subject’s request was forwarded to the Licensee. If the Data Subject request does not identify the sender’s Data Controller, Respondus will send Data Subject a generic reply with instructions to contact their Data Controller with their request.

To the extent permissible by law, Respondus shall promptly inform the Licensee, and in any case no later than (2) business days after receipt of any communication from (a) a Supervisory Authority in

connection with Personal Data processed under this Agreement, or (b) any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law.

Data Protection Impact Assessment

Upon Licensee's written request and to the extent that Licensee does not otherwise have access to the relevant information and the information is available to Respondus, Respondus shall provide Licensee with reasonable assistance (at Licensee's cost) needed to fulfill the Licensee's obligations under the Applicable Data Protection Law to carry out a data protection impact assessment related to Licensee's use of the Service. Such assistance may include:

A systematic description of the envisaged processing operations and the purpose of the processing;

An assessment of the necessity and proportionality of the processing operations in relation to the Services; and

The measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

To the extent necessary, Respondus shall provide reasonable assistance to the Licensee in the consultation with its relevant Supervisory Authority.

Security Incidents

If Respondus becomes aware of an actual Security Incident leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Licensee Data, Respondus will: (a) notify Licensee of the Security Incident without undue delay; (b) take appropriate steps to identify the cause of the Security Incident, minimize harm and secure the Licensee Data; and (c) provide Licensee with information as may be reasonably necessary to assist Licensee with its notification and reporting responsibilities.

The obligation for Respondus to notify under this clause shall include the provision of further information to the Licensee in phases, as details become available.

Respondus will not evaluate the contents of the Licensee Data to identify any specific reporting or other legal obligations that are applicable to the Licensee. Any and all regulatory and/or Data Subject reporting obligations related to the Security Incident are the responsibility of the Licensee. Respondus' notification of or response to a Security Incident under this DPA will not be construed as an acknowledgement by Respondus of any liability or fault with respect to the Security Incident.

Records of Processing

Respondus shall maintain a written record, even digitally, of all Processing carried out on behalf of the Licensee, in accordance with the provisions under Article 30 of the GDPR. Upon request, and at the expense of the Licensee, Respondus shall also provide an extract, whether complete or partial, of the record.

The Licensee may make such record available to the Supervisory Authority.

Audit

Respondus shall maintain complete and accurate records and information to demonstrate its compliance with this DPA and shall make such records available for audit by Licensee or any regulatory authority having jurisdiction. In particular, Respondus shall respond to written audit questions submitted by Licensee or the Licensee's designated auditor related to Respondus' processing and protection of Licensee Data. Licensee shall not exercise this right more than one time per year, and all audits shall be performed at Licensee's expense.

Retention/Deletion

At all times during the Term, Licensee will have the ability to access the Licensee Data. Respondus will retain Licensee Data for the period of time described in the Documentation. If the subscription is terminated, Respondus will disable Licensee's access to the Licensee Data. Access can be restored within the retention period by reinstating a valid subscription. The Licensee Data will be deleted at the end of the retention period, unless Respondus is permitted or required by applicable law, or authorized under this DPA, to retain such data.

Data Deletion

Upon completion of the processing-related services and/or upon termination of all Processing activities, for any reason, and in any case, no later than the expiry date of this Appointment, and contingent upon the request of the Licensee, Respondus shall destroy all Personal Data processed on behalf of the Licensee, unless a further period of time is provided for the storage of Personal Data under a provision of applicable law. Upon request, Respondus shall provide a written statement confirming the erasure of the Licensee Data along with the erasure all existing copies of the Licensee Data, within and no later than 7 (seven) days from the deletion of the Licensee Data.

US Privacy Shield

Respondus will provide at least the same level of protection for the Licensee Data as is required under the Privacy Shield, and shall promptly notify Licensee if it makes a determination that it can no longer provide this level of protection. In such event, or if Licensee otherwise reasonably believes that Respondus is not protecting the Licensee Data as required under the Privacy Shield, Licensee may either: (a) instruct Respondus to take reasonable and appropriate steps to stop and remediate any unauthorized processing, in which event Respondus shall promptly cooperate with Licensee in good faith to identify, agree and implement such steps; or (b) terminate this DPA and the Agreement without penalty by giving notice to Respondus.

General Terms

Confidentiality

Each Party must keep this Agreement and information it receives about the other Party and its business in connection with this Agreement ("Confidential Information") confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the

extent that: (a) disclosure is required by law; (b) the relevant information is already in the public domain.

Notifications

The Licensee may send notifications and communications under the terms of the DPA to Respondus at the following email address: privacy@respondus.com

Notifications and communications by Respondus to the Licensee will be sent via email to the License Administrator registered with Respondus, or as designated by the Licensee.

ANNEX 1
STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

The entity indentified as “Licensee” in the DPA
(the **data exporter**)

And

Respondus, Inc.
PO Box 3247, Redmond, WA 98073, USA
Tel: +1 425 497 0389
E-mail: privacy@respondus.com
(the **data importer**)

each a ‘party’; together ‘the parties’,

have agreed on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1
Definitions

For the purposes of the Clauses:

- (a) ‘personal data’, ‘special categories of data’, ‘process/processing’, ‘controller’, ‘processor’, ‘data subject’ and ‘supervisory authority’ shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data¹;
- (b) ‘the data exporter’ means the controller who transfers the personal data;
- (c) ‘the data importer’ means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country’s system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
- (d) ‘the sub-processor’ means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
- (e) ‘the applicable data protection law’ means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
- (f) ‘technical and organizational security measures’ means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2
Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3
Third-party beneficiary clause

1 The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

¹ Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

2 The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3 The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

4 The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4 **Obligations of the data exporter**

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organizational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5 **Obligations of the data importer²**

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organizational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

² Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

- (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;
 - (ii) any accidental or unauthorized access; and
 - (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorized to do so;
- (e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
- (f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
- (g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
- (h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;
- (i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;
- (j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 6 **Liability**

1 The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

2 If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

3 If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1 The data importer agrees that if the data subject invokes against its third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2 The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1 The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2 The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3 The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9
Governing law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10
Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11
Sub-processing

1 The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses³. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

2 The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

3 The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4 The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

³ This requirement may be satisfied by the sub-processor co-signing the contract entered into between the data exporter and the data importer under this Decision.

Clause 12

Obligation after the termination of personal data-processing services

1 The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2 The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

Appendix 1 to the Standard Contractual Clauses

Data exporter

The data exporter is the legal entity specified as Licensee for the Respondus products. The data exporter's activities which are relevant to the restricted transfer are the provision of educational student assessment. The data exporter has licensed the software solution of the data importer for this purpose.

Data importer

The data importer is Respondus, Inc., a United States based provider of automated proctoring software, which processes personal data of the data exporter using an online interactive database of video/audio recordings and associated data featuring student activity captured during student assessment, in a cloud-based storage solution hosted in the USA.

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

- Students enrolled in the customer's institution or program
- Employees of the customer.

Categories of data

- **Authentication data** (user name)
- **Basic personal data** (first name, last name)
- **Contact information** (email address is optional - may be provided by students when obtaining technical support or making general inquiries)
- **Unique identification numbers and signatures** (student ID card is optional, depending on Licensee's operational requirement)
- **Pseudonymous identifiers** (student ID code assigned by LMS, if applicable)
- **Photos, video and audio** (video/audio recording of the examinee; a photo image of the examinee is optional, depends on Licensee's operational requirement)
- **Education data** (Proctoring Analysis: Analysis data from exam session, such as duration of exam or time spent per question, or flags indicating possible exam rule violations.)
- **Device identification** (IP address)

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

Not applicable

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

- Receiving data, including collection
- Holding data, including storage
- Using data, including analyzing
- Protecting data, including restricting, encrypting and security testing
- Returning data to the data exporter or data subject
- Erasing data, including destruction and deletion.

**Appendix 2
to the Standard Contractual Clauses**

Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

The data importer will maintain administrative, physical and technical safeguards for the protection of the security, confidentiality and integrity of Personal Data uploaded for the operation of the licensed products by the data exporter. Details regarding these safeguards are available on the Respondus Monitor HECVAT form, which is available upon request via URL: <https://web.respondus.com/hecvat/>

The sub-processor's administrative, physical and technical safeguards are described in their DPA, available via URL: https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf

INDEMNIFICATION CLAUSE

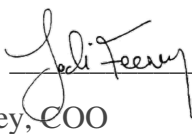
Liability

The parties agree that if one party is held liable for a violation of the clauses committed by the other party, the latter will, to the extent to which it is liable, indemnify the first party for any cost, charge, damages, expenses or loss it has incurred.

Indemnification is contingent upon:

- (a) the data exporter promptly notifying the data importer of a claim; and
- (b) the data importer being given control of the defense and settlement of the claim.

Signing the Standard Contractual Clauses, Appendix 1 and Appendix 2 on behalf of the data importer:

Signature  _____
Jodi Feeney, COO

Respondus, Inc.

PO Box 3247, Redmond, WA 98073, USA

ANNEX 2
SUB-PROCESSORS

The following Sub-Processors are approved by the Controller:

Name of Company

Amazon Web Services

Location of Processing

United States

Type of Processing

Data Hosting Server

Security Safeguards

Refer to AWS GDPR Data Processing Addendum

https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf