

Respondus Data Processing Agreement

Effective August 25, 2023

This Data Processing Agreement (“DPA”) is incorporated by reference and supplements the Respondus *LockDown Browser License Agreement for Educational Institutions* (the “License Agreement”), the Respondus Monitor Institution License and Terms of Use (“Terms”) and the Respondus Privacy Policy and any and all agreements governing Respondus Services (defined below) 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 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 or in the License Agreement, 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- (i) GDPR and any applicable national data protection laws, as may be amended or superseded from time to time;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.

“**Controller-to-Processor Clauses**” means the 2021 Standard Contractual Clauses between controllers and processors, specifically Module 2, for data transfers, as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 and incorporated by reference herein.

“**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/>.

“**EU-U.S. Data Privacy Framework**” means the EU-U.S. Data Privacy Framework self-certification program operated by the U.S. Department of Commerce and approved by the European Commission pursuant to Decision C (2023) 4745 of July 10, 2023.

“**FDPA**” means the Swiss Federal Data Protection Act including its implementing ordinances (Bundesgesetz über den Datenschutz), or any succeeding Swiss data protection law.”

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

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

“Service” **“Software 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 the Controller-to-Processor Clauses defined above. The SCC’s associated with this agreement may be found at <https://web.respondus.com/data-processing-SCCEUEAA>

“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.

“Swiss Addendum” means the supplementary document to this DPA, applicable when the FDPA applies to the Licensee’s use of the Services to process Swiss Licensee Data. The Swiss Addendum associated with this DPA may be found at <https://web.respondus.com/switzerland-dpa-addendum/>

Data Processing

Relationship of the Parties

The parties acknowledge and agree 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

As described above, Licensee is the Controller and Respondus is the Processor. Licensee (including its authorized staff and agents) use 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 to provide the Services to Licensee as Licensee’s Processor. 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 applicable law.

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 Licensee 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 Framework Requirements and industry standards.

Security

Respondus has implemented and will 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/ at least 30 days before the new Sub-Processor begins active work. 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 within 10 days of receipt of such notice from Respondus, 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 and to comply with applicable requirements related to data transfers including TIAs. 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-U.S. Data Privacy Framework, or to a recipient that has executed standard contractual clauses adopted or approved by the European Commission or other applicable data protection authority.

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 of Licensee 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 promptly if it considers that any of the Licensee's instructions infringe the Applicable Data Protection Law.

Direct Requests

Should a Data Subject of Licensee 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 and that Licensee's privacy, security, and related policies govern such requests. 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. If Respondus receives a valid Binding order from a governmental body for disclosure of Licensee Data, Respondus will use reasonable efforts to redirect the requesting party to request Licensee Data directly from Licensee.

To the extent permissible by law, Respondus shall promptly inform the Licensee, and in any case no later than two (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 and Prior Consultation

For the avoidance of doubt, Licensee is the Controller and is responsible for all their requirements under Applicable Data Protection Laws, including but not limited to its obligations to conduct a Data Protection Impact Assessment (DPIA), TIAs, and to respond to data subject requests. 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 as Controller under the Applicable Data Protection Law to carry out a DPIA and prior consultation related to Licensee's use of the Service. As Processor, Respondus' 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 as a Processor shall provide reasonable assistance to the Licensee in the consultation with its relevant Supervisory Authority.

Security Incidents

If Respondus becomes aware of an actual and confirmed 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, to the extent feasible and as details become available to Respondus.

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.

Notification(s) of Security Incidents, if any, will be delivered to Licensee's Administrative contacts by method of Respondus' choosing, including email. It is Licensee's sole responsibility to ensure its Administrative Contacts are up to date with Respondus and maintain secure transmission at all times.

Records of Processing

Respondus shall maintain a record 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 and subject to a nondisclosure agreement.

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, in alignment with Licensee's elected data retention period, or 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.

EU-U.S. Data Privacy Framework

Respondus will provide at least the same level of protection for the Licensee Data as is required under the EU-U.S Data Privacy Framework, 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 EU-U.S Data Privacy Framework, 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.

No Restriction of Rights

Nothing in this Agreement restricts Licensee's Data Subjects from exercising their rights under the GDPR.

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.

Termination of the DPA

This DPA will continue in force until the termination of the License Agreement (the "Termination Date").

Entire Agreement; Incorporation

When applicable, this DPA incorporates the Standard Contractual Clauses by reference. Nothing in this document varies or modifies the Standard Contractual Clauses.