

Honorlock

Data Processing Agreement

This Data Processing Agreement, including its Appendices and Annexes (collectively, the “**DPA**”) is entered into between Honorlock Inc. (“**Honorlock**,” “**we**” “**us**” or “**our**”), and your company (“**you**” or “**Subscriber**”); each, a “**Party**” and collectively, the “**Parties**”.

Recitals

- A. Subscriber and Honorlock have entered or will enter into an End User License Agreement (“**EULA**” or “**Agreement**”), which specifies the terms under which you may access and use the Services (as defined in the Agreement) provided by Honorlock. In delivering Services under the Agreement, Honorlock may Process Personal Data controlled by Subscriber.
- B. Honorlock is required to comply with Applicable Data Protection Laws when Processing Personal Data on behalf of Subscribers. Honorlock’s provision of Services to Subscriber pursuant to the Agreement is conditioned upon Subscriber entering into this DPA.

Terms and Conditions

1. Interpretation and Definitions

- 1.1 Unless otherwise defined herein, all capitalized words and expressions will have the same meanings assigned in the Agreement. In the event of any conflict or inconsistency between this DPA and the Agreement, the terms of this DPA shall control to the extent of any conflict or inconsistency.
- 1.2 “**Applicable Data Protection Laws**” means, as applicable, (i) State Data Protection Laws; (ii) European Data Protection Laws; and/or (iii) any other laws, rules, and regulations relating to the privacy, security, protection, and/or Processing of Personal Data, in each case as amended, superseded, or replaced.
- 1.3 “**Data Breach**” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data, or as otherwise defined in Applicable Data Protection Laws.
- 1.4 “**Data Subject**” means any natural person who can be identified, directly or indirectly, by reference to that person’s Personal Data including, as applicable, “**Consumers**” as defined under Applicable Data Protection Laws.
- 1.5 “**Data Subject Rights**” means certain rights granted to Data Subjects under Applicable Data Protection Laws regarding their own Personal Data.

- 1.6 **“DP Regulator”** means any local, state, provincial, national or multinational governmental or supervisory authority or regulatory body with competent jurisdiction to promulgate, administer, and/or enforce Applicable Data Protection Laws.
- 1.7 **“European Data Protection Law(s)”** means (i) 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) (**“EU GDPR”**); (ii) all laws relating to data protection, the Processing of personal data, privacy and/or electronic communications in force from time to time in the United Kingdom including the U.K. Data Protection Act 2018, Privacy and Electronic Communications (EC Directive) Regulations 2003 and the GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (**“UK GDPR”**) (collectively with the EU GDPR, the **“GDPR”**); (iii) the EU e-Privacy Directive (2002/58/EC); (iv) any national data protection laws made under or pursuant to (i), (ii) or (iii); and (v) the Swiss Federal Data Protection Act (**“Swiss DPA”**), in each case as superseded, amended or replaced, provided that, in the event of a conflict in the meanings of defined terms in the European Data Protection Laws, the meaning from the law applicable to the location of the relevant Data Subject shall apply.
- 1.8 **“Person”** means, as applicable, any natural person, corporation, limited liability company, general partnership, limited partnership, proprietorship, other business organization, trust, union, association, or governmental authority.
- 1.9 **“Personal Data”** or **“Personal Information”** means any information relating to an identified or identifiable natural person, or as otherwise defined in Applicable Data Protection Laws, that is Processed by Honorlock in connection with the Agreement and this DPA.
- 1.10 **“Process,” “Processing,”** or **“Processed”** means any operation or set of operations that is or may be performed on Personal Data (whether or not by automated means), or as otherwise defined in Applicable Data Protection Laws.
- 1.11 **“Restricted Transfer”** means (i) where the EU GDPR applies, a transfer of Personal Data from the European Economic Area (**“EEA”**) to a country outside of the EEA which is not subject to an adequacy determination by the European Commission; (ii) where the UK GDPR applies, a transfer of Personal Data from the United Kingdom to any other country which is not based on adequacy regulations pursuant to the UK GDPR; (iii) where the Swiss DPA applies, a transfer of Personal Data from Switzerland to any other country which is not subject to an adequacy decision by the Swiss Federal Data Protection and Information Commissioner; or (iv) as otherwise defined in Applicable Data Protection Laws.
- 1.12 **“Sensitive Data”** means any Personal Data that is defined as sensitive personal data, sensitive personal information, or equivalent term in Applicable Data Protection Laws.
- 1.13 **“Standard Contractual Clauses”** means where the EU GDPR applies, the standard contractual clauses annexed to the European Commission's Implementing Decision

2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (Module II: Controller to Processor), (“EU SCCs”), as supplemented by this DPA.

- 1.14 “**State Data Protection Laws**” means, collectively, all U.S. state data protection laws and their implementing regulations, as amended or superseded from time to time, that apply generally to the Processing of Personal Data related to Consumers and/or Households, in each case as superseded, amended, or replaced, *provided that*, in the event of a conflict or inconsistency in the meanings of defined terms in the State Data Protection Laws, the meaning from the law applicable to the state of residence of the relevant Consumer, or the state where the relevant Household is located, shall apply.
- 1.15 “**Subprocessor**” means any Person engaged directly or indirectly by Honorlock to Process any Personal Data relating to the Agreement and this DPA. The term “Subprocessor” shall also include any Person engaged directly or indirectly by a Subprocessor to Process any Personal Data relating to the Agreement and this DPA.
- 1.16 “**Technical and Organizational Security Measures**” means measures aimed at safeguarding Personal Data, including prevention of Data Breaches, or as otherwise specified in Applicable Data Protection Laws.
- 1.17 “**UK IDT Addendum**” means the UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (version 21, March 2022) laid before Parliament in accordance with s119A of the Data Protection Act 2018, as superseded, amended, or replaced.
- 1.18 “**UK International Data Transfer Agreement**” means the International Data Transfer Agreement (Version A1.0, in force 21 March 2022) laid before Parliament in accordance with S119A of the Data Protection Act 2018, as superseded, amended, or replaced.
- 1.19 The terms **Notice of Collection, Business, Service Provider, Contractor, Third Party, Controller, Processor, Sell, and Share** (capitalized or lowercase) have the meanings set forth in Applicable Data Protection Laws.

2. **Processing Activities**

- 2.1 Honorlock shall (i) Process Personal Data in accordance with the Agreement and this DPA only as a Processor, Service Provider or Contractor as instructed by Subscriber, and on behalf of Subscriber; and (ii) comply with its obligations under Applicable Data Protection Laws. At Subscriber’s reasonable request, Honorlock shall make available to Subscriber and/or DP Regulators all information in its possession or under its control necessary to demonstrate its compliance with Applicable Data Protection Laws. Honorlock shall not collect, use, retain, disclose or otherwise Process the Personal Data for its own purposes or those of any third party (including, without limitation, by creating or maintaining data which is derived from Personal Data, or anonymizing or de-identifying Personal Data). Annex A to this DPA describes the scope, nature, and purpose of Processing by Honorlock, the duration of Processing, the types of Personal Data, and the categories of Data Subjects.

2.2 Honorlock shall immediately inform Subscriber if, in Honorlock's opinion, an instruction infringes Applicable Data Protection Laws, or if Honorlock determines that it cannot comply with its obligations under this DPA or Applicable Data Protection Laws. In such event, Honorlock shall work with Subscriber and take all reasonable and appropriate steps to stop any Processing until such time as the Processing complies with such requirements. Honorlock shall immediately cease (and instruct its Subprocessors to cease) Processing Personal Data if Subscriber determines that Honorlock has not or cannot correct any such non-compliance within a reasonable time frame.

2.3 Honorlock will (and ensure that its Subprocessors will) Process the Personal Data in compliance with this DPA and Applicable Data Protection Laws.

3. Technical and Organizational Security Measures

3.1 Any Person authorized by Honorlock to Process the Personal Data for Subscriber will be subject to a duty of confidentiality (contractual, statutory or otherwise) and will Process the Personal Data only for the purpose of delivering the Services to Subscriber under the Agreement and this DPA, and/or any third party as agreed therein.

3.2 Honorlock will implement and maintain the Technical and Organizational Security Measures identified in Annex B, which are designed to safeguard and preserve the security, integrity, and confidentiality of Personal Data and protect the Personal Data from Data Breaches in accordance with Applicable Data Protection Laws.

4. Cooperation

4.1 Honorlock shall cooperate with Subscriber to enable Subscriber to respond to any requests, complaints or other communications from Data Subjects, DP Regulators, or judicial bodies relating to the Processing of Personal Data under the Agreement, including Data Subject Requests. If any such request, complaint or communication is made directly to Honorlock, Honorlock shall promptly notify Subscriber, providing a copy of the relevant communication, and shall not respond to such communication without Subscriber's prior express written authorization unless required to do so under applicable law.

4.2 If Honorlock receives a subpoena, court order, warrant or other legal demand from a third party (including law enforcement or other public or judicial authorities) seeking the disclosure of Personal Data, Honorlock will promptly notify Subscriber in writing of such request, providing a copy of the relevant communication, and reasonably cooperate with Subscriber if it wishes to limit, challenge or protect against such disclosure, to the extent permitted by applicable law.

4.3 To the extent required under Applicable Data Protection Laws, Honorlock will assist Subscriber to conduct a data protection impact assessment or equivalent and, where legally required, consult with applicable DP Regulators in respect of any proposed or modified Processing activity that presents a high risk to Data Subjects or requires such an assessment under Applicable Data Protection Laws.

5. Data Protection

5.1 Pursuant to and in compliance with this DPA, Honorlock hereby agrees:

- (i) Where Subscriber is regulated by State Data Protection Laws and the Personal Data Processed by Honorlock pursuant to the Agreement and this DPA relate to Data Subjects that reside in the United States of America (“USA”), or Households located in the State of California, USA, then Honorlock shall Process such Personal Data in compliance with Part A of Appendix 1 to this DPA; and
- (ii) Where Subscriber is regulated by the European Data Protection Laws and the Personal Data Processed by Honorlock pursuant to the Agreement and this DPA relate to Data Subjects located in the EEA, the United Kingdom or Switzerland, then Honorlock shall Process such Personal Data in compliance with Part B of Appendix I to this DPA.

5.2 Where Subscriber is regulated by Applicable Data Protection Laws in other countries, and the Personal Data Processed by Honorlock pursuant to the Agreement and this DPA relates to Data Subjects that are residents of or located in such other countries, then Honorlock shall Process such Personal Data in compliance with such other Applicable Data Protection Laws, provided that, such compliance does not impose on Honorlock any new, material or additional obligations, costs, or expenses.

6. Subprocessors

6.1 Honorlock has Subscriber’s authorization to engage any Subprocessors from the list provided in Annex C.

6.2 Honorlock may engage new Subprocessors not listed in Annex C, provided that:

- (i) Honorlock provides at least ten (10) days prior written notice to Subscriber of the engagement of any new Subprocessor (including details of the Processing and location), thereby giving Subscriber sufficient time to be able to object to such changes prior to the engagement of the Subprocessor, and Honorlock shall update the list of all Subprocessors engaged to Process Personal Data under this DPA in Annex C and send such updated version to Subscriber prior to the engagement of the new Subprocessor;
- (ii) Honorlock imposes the same data protection terms on any Subprocessors it engages as contained in this DPA (including the Standard Contractual Clauses and/or other data transfer provisions, where applicable); and
- (iii) Honorlock remains fully liable for any breach of this DPA or the Agreement that is caused by an act, error or omission of such Subprocessors.

6.3 If Subscriber reasonably objects to Honorlock’s engagement of a new Subprocessor pursuant to Section 6.2 on data protection grounds, then either Honorlock will not engage the Subprocessor to Process the Personal Data or Subscriber may elect to suspend or

terminate the Processing of Personal Data under the Agreement in whole or in part and without penalty.

7. Data Breach

- 7.1 Honorlock shall (i) notify Subscriber without undue delay after becoming aware of a Data Breach; (ii) investigate and undertake to remediate the Data Breach; and (iii) provide Subscriber with all reasonably requested information regarding the Data Breach, including any information necessary to comply with its notification and other obligations under Applicable Data Protection Laws.
- 7.2 Honorlock's notification under Section 7.1 shall include, to the extent available, information regarding: (i) the nature of the Data Breach; (ii) the types of Personal Data impacted by the Data Breach, and the Data Subjects whose Personal Data was impacted; (iii) likely consequences of the Data Breach; and (iv) the measures taken to address the Data Breach. Honorlock will update the notification as additional information becomes available.
- 7.3 Unless required to do so under applicable law, Honorlock shall not notify any Data Subjects, DP Regulators, law enforcement or governmental authorities without, in each instance, Subscriber's prior written authorization, and Subscriber shall, at its discretion, determine any notifications (including content and timing thereof), required of Subscriber by Applicable Data Protection Laws.

8. Audits

- 8.1 While it is the Parties' intention ordinarily to rely on Honorlock's obligations set forth in Section 5 to verify its compliance with this DPA, Subscriber (or its appointed representatives) may carry out an inspection of Honorlock's operations and facilities (limited in scope to operations and facilities that Process Personal Data on behalf of Subscriber) during normal business hours and subject to reasonable prior notice of at least ten (10) business days where Subscriber considers it necessary or appropriate (for example, without limitation, where Subscriber has reasonable concerns about Honorlock's data protection compliance following a Data Breach or following instruction from a DP Regulator). Any such inspection shall (i) be conducted at Subscriber's sole cost and expense, (ii) not unduly interfere with Honorlock's business, and (iii) respect Honorlock's confidentiality and privacy obligations to its other customers.

9. Effect of Termination

- 9.1 This DPA shall (i) commence on the Effective Date of the Agreement and remain in effect until no Personal Data remains in the possession or control of Honorlock or its Subprocessors; and (ii) survive expiration or termination (for any reason) of the Agreement. The termination or expiry of any Processing of Personal Data by Honorlock or its Subprocessors shall be without prejudice to any accrued rights or remedies of either Party under this DPA at the time of such termination or expiration.

- 9.2 Upon Subscriber's request at any time, and/or at Subscriber's direction upon termination or expiration of the Agreement or this DPA, Honorlock shall (at Subscriber's choice) destroy or return to Subscriber all Personal Data (including copies) in its possession or control. This requirement shall not apply to the extent that (i) Honorlock is required by applicable law to retain some or all of the Personal Data, and/or (ii) electronic copies of Personal Data are stored in automated backups or archives; in which event Honorlock shall isolate and protect the Personal Data using the Technical and Organizational Security Measures required by this DPA and not Process the Personal Data except to the extent required by such applicable law.

10. General

- 10.1 Any limitations and exclusions of liability or damages set out in the Agreement shall apply to and limit a Party's liability to the other Party arising directly or indirectly out of or in connection with a breach of this DPA and/or the Applicable Data Protection Laws by such Party or by other parties for which such Party is responsible under this DPA unless (i) a court of competent jurisdiction determines otherwise pursuant to a final, non-appealable judgement, or (ii) such limitations as set forth in the Agreement are otherwise prohibited under the Applicable Data Protection Laws.
- 10.2 If any part of this DPA is held unenforceable, the validity of all remaining parts will not be affected. This DPA may not be modified except by a subsequent written instrument signed by both Parties.
- 10.3 To the extent required by Applicable Data Protection Laws, this DPA shall be governed by the law of the applicable jurisdiction. In all other cases, this DPA shall be governed by the law of the same jurisdiction as the Agreement.
- 10.4 This DPA (including Recitals, Terms and Conditions, Appendices, and Annexes, each hereby incorporated by reference) is the entire agreement of the Parties with respect to its subject matter.

Data Protection Agreement

Appendix I – Part A

State Data Protection Laws

1. Scope and Roles of the Parties

- 1.1 The Parties acknowledge and agree that under State Data Protection Laws, Subscriber is the Controller or Business, as applicable, and Honorlock is the Processor or Service Provider, as applicable, for purposes of Processing the Personal Data in accordance with the Agreement and this DPA.
- 1.2 Honorlock shall (i) comply with this DPA and State Data Protection Laws, (ii) provide the same or higher level of privacy and cybersecurity protection for the Personal Data as required by the State Data Protection Laws, and (iii) provide Subscriber with all reasonably requested cooperation, assistance and information to enable Subscriber to fulfill its own obligations under State Data Protection Laws.
- 1.3 Subscriber has the right to (i) take reasonable and appropriate steps to ensure that Honorlock Processes Personal Data consistent with Subscriber's obligations under State Data Protection Laws; (ii) monitor Honorlock's compliance with this DPA and State Data Protection Laws through measures, including, but not limited to, ongoing manual reviews, automated scans, regular assessments, audits, or other annual technical and operational testing at least once every 12 months; and (iii) stop and remediate unauthorized Processing of Personal Data after receiving notice or otherwise becoming aware that Honorlock and/or any Subprocessor can no longer meet its or their obligations pursuant to this DPA and/or applicable State Data Protection Laws.
- 1.4 In order to confirm its compliance with this DPA and its obligations under State Data Protection Laws, Honorlock shall permit Subscriber to conduct, and shall reasonably cooperate with Subscriber in connection with, (i) ongoing manual reviews and automated scans of its access, collection, use and/or other Processing of Personal Data, and (ii) at least once every twelve (12) months, regular assessments, audits or other technical and operational testing thereof.

2. Restrictions on Processing

- 2.1 Honorlock is prohibited from (i) Selling (as defined under Applicable Data Protection Laws) or Sharing (as defined under the CPRA) Personal Data, (ii) retaining, using, or disclosing Personal Data for any purpose other than for the specific purpose of performing and/or providing the Services specified in the Agreement; (iii) retaining, using, or disclosing Personal Data outside of the direct business relationship between the Parties except as required under applicable law; and (iv) combining Personal Data with Personal Data obtained from, or on behalf of, sources other than Subscriber (unless specific statutory or regulatory exceptions apply).

- 2.2 The Parties acknowledge and agree that the transfer and/or exchange of the Personal Data between the Parties does not form part of any monetary or other valuable consideration exchanged between the Parties with respect to the Agreement or this DPA.
- 2.3 Notwithstanding any provision to the contrary of the Agreement or this DPA, the terms of this DPA shall not apply to Honorlock's Processing of Personal Data that is excluded from State Data Protection Laws.

3. Conflicts

In the event of any conflict or inconsistency between this Part A of Appendix 1 and the DPA, Part A of Appendix 1 shall govern and control with respect to its subject matter.

Data Protection Agreement

Appendix I – Part B

European Data Protection Laws

1. Scope and the Roles of the Parties

- 1.1 The Parties acknowledge and agree that for the purposes of the European Data Protection Laws, Subscriber is the Controller and Honorlock is the Processor for purposes of Processing the Personal Data in accordance with the Agreement and this DPA.
- 1.2 Honorlock shall only process the Personal Data on the documented instructions of Subscriber unless Honorlock is required by the European Data Protection Laws to otherwise process Personal Data.
- 1.3 For purposes of Section 1.2, Subscriber hereby instructs the Honorlock to Process the Personal Data for the purpose of delivering the Services to Subscriber in accordance with the Agreement and this DPA.

2. Restricted Transfers

- 2.1 Honorlock shall not Process or transfer any Personal Data in or to a country or jurisdiction other than the country or jurisdiction in which the Personal Data was first collected (nor permit the Personal Data to be so Processed or transferred) unless: (i) it has first obtained Subscriber's prior written consent; and (ii) it takes the measures necessary to ensure such Processing or transfer is in compliance with European Data Protection Laws (including such measures as may be communicated by Subscriber to Honorlock).
- 2.2 The Parties agree that the EU SCCs are hereby incorporated into and form an integral part of this DPA where and to the extent of any Restricted Transfer pursuant to the EU GDPR. The Parties agree that (i) Subscriber shall be deemed the "data exporter" and Honorlock shall be deemed "data importer"; (ii) in Clause 7, the optional docking clause will not apply; (iii) in Section 9, option 2 will apply; (iv) in Clause 11, the optional language will not apply; (v) in Clause 17, Option 1 will apply, and the SCCs will be governed by the laws of the Republic of Ireland; (vi) in Clause 18(b), disputes shall be resolved before the courts of the Republic of Ireland; (vii) Annex I of the EU SCCs shall be deemed completed with the information set out in Annex A to this DPA; (viii) Annex II of the EU SCCs shall be deemed completed with the information set out in Annex B to this DPA; and (ix) Annex III of the EU SCCs shall be deemed completed with the information set out in Annex C to this DPA.
- 2.3 If the EU SCCs apply to a Restricted Transfer originating from the United Kingdom, this Section shall apply to and modify the EU SCCs to the extent that the UK GDPR applies. The Parties acknowledge and agree that: (i) the information required to be set forth in "Part 1: Tables of the UK IDT Addendum shall be completed in accordance with Annex A, Annex B and Annex C; and (ii) "Part 2: Mandatory Clauses" of the UK IDT Addendum, as it is revised under Section 18, is hereby incorporated herein by reference. For purposes

of Section 19 of the UK IDT Addendum, Subscriber may end the UK IDT Addendum in accordance with Section 19 thereof.

- 2.4 If the Restricted Transfer originates only from the United Kingdom, then the Parties may use the UK International Data Transfer Agreement. The Parties acknowledge and agree that Annexes A, B and C will be appended to the UK International Data Transfer Agreement.
- 2.5 In the case of Restricted Transfers of Personal Data protected by Swiss law, the EU SCCs shall apply subject to the following amendments: (i) references to “Regulation (EU) 2016/679” will be deemed to refer to the Swiss DPA; (ii) references to specific articles of “Regulation (EU) 2016/679” will be deemed replaced with the equivalent article or section of the Swiss DPA; (iii) references to “EU,” “Union,” and “Member State” will be deemed replaced with “Switzerland”; (iv) references to the “competent supervisory authority” are replaced with the “Swiss Federal Data Protection Information Commissioner”; and (v) in Clause 18(b), disputes shall be resolved before the competent courts of Switzerland.
- 2.6 It is not the intention of either Party, nor the effect of this DPA, to contradict or restrict any of the provisions set forth in the EU SCCs as supplemented herein. Accordingly, if and to the extent the EU SCCs as supplemented herein conflict with any provision of this DPA, the EU SCCs as supplemented herein shall prevail. In no event does this DPA restrict or limit the rights of any Data Subject or of any competent supervisory authority.
- 2.7 The Parties agree that in the event that European Data Protection Laws and/or a regulator no longer allow the lawful transfer of Personal Data to Honorlock and/or require that Subscriber adopt an alternative data transfer mechanism to that relied upon this Section to ensure an adequate level of protection for Personal Data, the Parties will negotiate in good faith to enter into an amendment to this DPA to remedy such non-compliance and, where required by Subscriber, immediately cease (and instruct all Subprocessors to immediately cease) all Processing of Personal Data until such agreement is reached. If the Parties, acting in good faith, are unable to come to an agreement within 30 days, each Party may immediately terminate the Agreement and this DPA without penalty.

3. Conflicts

In the event of any conflict or inconsistency between this Part B of Appendix 1 and the DPA, Part B of Appendix 1 shall govern and control with respect to its subject matter.

ANNEX A

DETAILS OF THE PROCESSING / TRANSFER

A. LIST OF PARTIES

Data exporter(s):

Name: [Subscriber]

Address: [Subscriber address as specified in the applicable Agreement(s)]

Contact person's name, position and contact details: [insert]

Activities relevant to the data transferred under these Clauses: As set out in the Agreement between the Parties.

Signature and date: As set out in the DPA.

Role (controller/processor): Controller.

Data importer(s):

Name: Honorlock, Inc. (“**Honorlock** ”)

Address: Honorlock 2500 North Military Trail, Suite 322, Boca Raton, Florida 33431, USA

Contact person's name, position and contact details: privacy@honorlock.com

Activities relevant to the data transferred under these Clauses: As set out in the Agreement between the Parties.

Signature and date: As set out in the DPA.

Role (controller/processor): Processor.

B. DESCRIPTION OF TRANSFER

Categories of Data Subjects whose personal data is transferred

Students, instructors.

Categories of personal data transferred

Student name, email, ID; student connection information; student face photo/ID images; student webcam recording; instructor name and email address; instructor exam and course information; school LTI keys and instructor OAuth keys.

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.

None.

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

Continuous during the term of the Agreement.

Nature of the processing

The Personal Data Processed by Honorlock and/or its Subprocessors will be subject to the Processing activities described in the Agreement subject to this DPA. Personal Data may be Processed only in order to comply with Subscriber's instructions issued in accordance with the DPA.

Purpose(s) of the data transfer and further processing

The purpose of the data Processing under this DPA is the provision of the Services by Honorlock to Subscriber as set out in the Agreement and in the table below.

Data	Purpose of Processing
Student name, email, ID	Identification of the student taking the exam
Student connection information	Identification of student location and computer/browser information while taking the exam session
Student face photo/ID images	Identification of the student taking the exam
Student webcam recording	Proctoring the exam and analyzing their session

Instructor name and email address	Assigning exam information and communication to the proctoring system
Instructor exam and course information	Proctoring the exam to the student in the course
School LTI keys and instructor OAuth keys	LMS integration and authentication

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

The duration of the data Processing under this DPA is until the termination or expiration of the Agreement in accordance with its terms.

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

See Annex C. The duration of the processing is the term of the engagement.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13 of the EU SCCs

Data Protection Commission (DPC) of the Republic of Ireland.

ANNEX B

TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

LMS Integrations

Honorlock integrates with Canvas, D2L, and Blackboard LMS using LTI 1.3 Standards and available REST APIs; Honorlock's Intellum integration utilizes Intellum APIs. When using Honorlock through the LTI or extension, no passwords are required to use Honorlock, the LTI integration uses single-sign-on authentication and is completely OAuth-based.

Hosting Provider Overview

Honorlock is an on-demand online proctoring solution with 24/7/365 availability. Cloud-computing (SaaS) infrastructure is provided by Amazon Web Services (AWS), including Amazon Elastic Compute Cloud (EC2), and fully redundant storage infrastructure of the Amazon Simple Storage Service (S3). Customer data is hosted by Amazon Web Services with multiple availability zones and backups are saved to another region. All data is processed and stored within the United States.

Organizational Security

A core tenet of Honorlock's security revolves around the policies and procedures we've put in place to ensure all of the Honorlock team members are protecting the data of our customers. All Honorlock employees must pass a background check and sign non-disclosure agreements prior to starting at Honorlock. They are also required to complete annual trainings on Information Security, Privacy, FERPA, Sexual Harrassment, and social engineering (including phishing). Developers participate in secure coding and general security best practices training. Beyond training, Honorlock regularly prepares for incidents and disaster recovery. Our incident response plan is focused on procedures to detect, respond to, and limit the effects of any incident. We test and confirm the success of our incident response plan and Business Continuity plans annually.

Infrastructure & Development

Honorlock takes a security-first approach in the infrastructure and development of the Honorlock application. All data is encrypted in transit and at rest using industry standard best practices. It is Honorlock's policy to follow the principle of least privilege. Privileged access must also be provisioned with the minimum amount of access possible to perform job functions and both are managed with Role-Based Access Control (RBAC). Honorlock's security monitoring ensures appropriate mechanisms are in place to secure systems and applications and are not bypassed. Additionally, Honorlock conducts routine third party vulnerability assessments, scans, and penetration testing to ensure data protection.

Authentication & Data

Honorlock is committed to protecting the privacy of all students and instructors. Honorlock is not the owner of the data but does hold the data for the institution; data retention periods are established within each customer's MSA. Employees do not have access to personal data unless their job requires it (e.g., support or proctors) and all employees complete training that covers the proper handling of data. Additional information on what is collected can be found in our Exam Taker

Privacy Notice (<https://honorlock.com/honorlock-privacy-policy/>). In order to take an exam, students are required to install the Honorlock Chrome extension. This extension requests access to read and change data on websites and capture the content of the user screen. The Honorlock extension is only active and recording information when an exam is in progress, and a visual indicator is available to notify the user that the extension is active.

ANNEX C

List of Honorlock's Subprocessors

Name:	Twilio
Address:	375 Beale Street, Suite 300, San Francisco, CA 94105
Contact person's name, position and contact details:	Tom Maddock. Partner Account Executive. tmaddock@twilio.com .
Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised):	Provides API integration tool for Service Provider's application.
Name:	AWS
Address:	410 Terry Avenue North, Seattle, WA 98109
Contact person's name, position and contact details:	
Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised):	Stores all of Service Provider's data
Name:	Olark
Address:	427 North Tatnall Suite 73055, Wilmington, DE 19801
Contact person's name, position and contact details:	Support@olark.com
Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised):	Live chat software. Provides tool for proctors to interact with customers.
Name:	Stripe
Address:	354 Oyster Point Blvd, South San Francisco, CA 94080
Contact person's name, position and contact details:	https://support.stripe.com/?contact=true
Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised):	Processes credit card transactions.

Name:	LiveChat
Address:	101 Arch Street, 8 th Floor, Boston, MA 02110
Contact person's name, position and contact details:	support@livechatinc.com
Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised):	Chat bot; provides support for customer interactions.