Honorlock Inc.
GDPR & Privacy Shield Notice
Effective Date: May 21, 2019

Scope of this GDPR & Privacy Shield Notice

This GDPR & Privacy Shield Notice is included in our App and Website Privacy Policies (the "Privacy Policies") and applies to the "personal data," as defined in the GDPR, of natural persons located in the European Economic Area ("EEA Individuals," "you," or "your"). Any capitalized terms or other terms not defined herein shall have the meaning ascribed to them elsewhere in the Privacy Policy or, if not defined herein or elsewhere in the Privacy Policies, the GDPR.

The term "European Economic Area" (or "EEA") shall mean the then-current member states and member countries of the European Union and European Economic Area, respectively, Switzerland, and, upon its withdrawal from the European Union, the United Kingdom.

With respect to any combination of conflict between the provisions of the GDPR Privacy Notice (the "GDPR Notice"), Privacy Shield Notice, and any other provision of the Privacy Policies, the following will control in order of precedence from highest to lowest (with (1) being the highest and (3) being the lowest) only with respect to EEA Individuals and their personal data: (1) the GDPR Notice, (2) the Privacy Shield Notice, and then (3) any other provision of the Privacy Policies.

GDPR Privacy Notice

Processor Disclosure: We are a data processor of the personal data processed through our Services (i.e., the proctoring services we provide through our App) ("App Data"), including the personal data of Students and Authorized Users and except as otherwise described in ***Controller Disclosure & Details***.

The App Data processed by Honorlock primarily depends on the features or functionality that Faculty requires its Students to use on the Services before commencing an Exam. App Data primarily includes:

- User and exam information pulled from the LMS that our Services are running on (e.g., unique LMS user ID, user name, user email, quiz name, course name);
- Proctoring reports of any alleged misconduct or violations;
- Timestamps of answered questions;
- Device Information (such as IP address, user agent string, network information) on Primary Devices and Secondary Devices (i.e., the computer used to take the Exam and other devices that may be in the room, respectively);
- Actions taken when a Student is taking an exam (e.g., copy/cut/right-click actions), including use of Secondary Devices (including their use on "honeypot" sites that purport to have Exam answers);
- Screen and webcam monitoring; and

- Authentication Data (i.e., data used to confirm the identity of the Student taking an Exam, such as webcam and ID photos)

When serving as a processor, we have certain obligations under GDPR including only processing personal data at our customers' instructions reflected in the applicable Master Services Agreement, providing assistance with fulfilment of rights requests, and implementing appropriate security for personal data. We will forward any inquiries, complaints, or requests received from data subjects with respect to App Data to the appropriate customer and await instructions before taking any further action.

Controller Disclosure & Details: We are a data controller of personal data regarding the following categories of EEA Individuals: Prospective/current customers (collectively, **"**Business Contacts") and Visitors for the purposes and under the legal bases described in the table below. Please note that, in some cases, the categories of data subjects above may overlap (e.g., Business Contacts using the Website are also Visitors).

Data Subject Category	Purpose & Legal Basis of Processing
General (applies to all data subjects below)	Information Security: Our web servers will log your IP address and other information (e.g., browser information, operating system, request date/time, user agent string, referral and exiting URL) in order to maintain an audit log of activities performed. We use this information pursuant to our legitimate interests in tracking Website and App usage, combating DDOS or other attacks, and removing or defending against malicious individuals or programs on the Website and App.
Business Contacts	Direct Marketing: Our legitimate interest in sending current or prospective customers email marketing; App Demonstrations: Our legitimate interest in setting up demos with prospective customers pursuant to their request; Executing Contracts and other Legal Documentation: We will process all personal data as necessary for the performance of contracts to which Business Contacts are a party (such as our Terms of Use or the Privacy Policies) or to take requested steps to enter into such contracts. General Business Development: Our legitimate interest in furthering business relationships (such as by storing Business Contact information within a CRM or other file), ensuring customer satisfaction, and answering inquiries.

EU Representative: Our representative in the European Union is:

GDPR-REP.eu
Maetzler Rechtsanwalts GmbH & Co KG

Attorney at Law
Schellinggasse 3/10, 1010 Vienna, Austria

https://gdpr-rep.eu/

Recipients: Honorlock personnel shall receive and process your personal data for the purposes described herein. Such personal data is also disclosed to the following recipients to effectuate the purposes described herein:

- Zoom: Video conferencing
- Google GSuite: Collaboration and productivity apps
- QuickBooks: Accounting system
- Salesforce: Customer Relationship Management (CRM)
- Slack: Internal communication tool
- Stripe: Payment processor
- YesWare: Sales productivity

Retention: Please see below for our general retention periods. Please note that the below retention periods may be extended or shortened, as appropriate, based on the context of our relationship with an EEA Individual (e.g., negotiations for a sale, interest in the App), and for compliance with legal obligations (e.g., accounting, finances, tax, establishment, exercise, or defense of legal claims).

Honorlock will retain the personal data related to our Business Contacts for a period no longer than seven (7) years, without prejudice to any request by a Business Contact to be removed earlier.

Personal data contained within contractual and other legal documentation shall be retained indefinitely (e.g., signatures).

Your GDPR Rights: As a natural person, you have a right to: (i) request access to, correction and/or erasure of your personal data; (ii) object to processing of your personal data; (iii) restrict processing of your personal data; and (iv) request a copy of your personal data, or have a copy thereof sent to another controller, in a structured, commonly used and machine readable format under the right of data portability. You may exercise these rights and submit a GDPR complaint by contacting: privacy@honorlock.com with the subject line "**GDPR Notice**."

You also have the right to lodge a complaint about the processing of your personal data with an appropriate data protection authority, and, as applicable, to exercise third-party beneficiary rights under Honorlock's Standard Contractual Clauses.

Objecting to Legitimate Interest/Direct Marketing: You may object to personal data processed pursuant to our legitimate interest. In such case, we will no longer process your personal data unless we can demonstrate appropriate, overriding legitimate grounds for the processing or if needed for the establishment, exercise, or defense of legal claims. You may also object at any time to processing of your personal data for direct marketing purposes by clicking "Unsubscribe"

within an automated marketing email or by submitting your request to privacy@honorlock.com with the subject line "**GDPR Notice**" (the latter for instances where, for example, you would not like to receive follow-ups from our sales team). In such case, your personal data will no longer be used for that purpose.

Transfer of Personal Data outside the EEA: We are self-certified under the EU-US and Swiss-US Privacy Shield for appropriate transfer of your personal data, such as to our US data centers, pursuant to Article 45(1); in these instances, you may have specific rights under the Privacy Shield (see ***E.U.-U.S. and Swiss-U.S. Privacy Shield Notice*** below). In other instances, however, we may alternatively rely on appropriate Standard Contractual Clauses to ensure adequate protection for your personal data.

Disclosure to Public Authorities: Honorlock may be required to disclose personal data in response to lawful requests by public authorities, including for the purpose of meeting national security or law enforcement requirements. We may also disclose personal data to other third parties when compelled to do so by government authorities or required by law or regulation including, but not limited to, in response to court orders and subpoenas.

***Corporate Restructuring*:** In the event of a merger, reorganization, dissolution or similar corporate event, or the sale of all or substantially all of our assets, we expect that the information that we have collected, including personal data, would be transferred to the surviving entity in a merger or the acquiring entity. All such transfers shall be subject to our commitments with respect to the privacy and confidentiality of such personal data as set forth in this GDPR Notice.

Updates to this GDPR Notice: If, in the future, we intend to process your personal data for a purpose other than that which it was collected, we will provide you with information on that purpose and any other relevant information at a reasonable time prior to such processing. After such time, the relevant information relating to such processing activity will be revised or added appropriately within this GDPR Notice, and the "Effective Date" at the top of this page will be updated accordingly.

How to Contact Us: Please reach out to privacy@honorlock.com for any questions, complaints, or requests regarding this GDPR Notice with the subject line, "**GDPR Notice**."

E.U.-U.S. and Swiss-U.S. Privacy Shield Notice

Note: For the avoidance of doubt, we separately mention Switzerland and United Kingdom for purposes of this Privacy Shield Notice.

Privacy Shield: If your personal information is transferred from the EEA, Switzerland, or the United Kingdom to the US pursuant to the Privacy Shield, then the rights, remedies and protections set forth in this section apply to you. We comply with the EU-US Privacy Shield Framework and the Swiss-US Privacy Shield Framework as set forth by the US Department of Commerce regarding the collection, use, and retention of personal data transferred from the European Union member countries (including Iceland, Liechtenstein, and Norway), Switzerland, and the United Kingdom, respectively, to the United States pursuant to the EU-US and Swiss-US

Privacy Shield. Honorlock has certified that we adhere to the Privacy Shield Principles with respect to such data. If there is any conflict between the policies in this Privacy Policy and data subject rights under the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification page, please visit https://www.privacyshield.gov/

With respect to personal data received or transferred pursuant to the Privacy Shield Frameworks, Honorlock is subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC).

In compliance with the Privacy Shield Principles, Honorlock commits to resolve complaints about your privacy and our collection or use of your personal information transferred to the United States pursuant to Privacy Shield. European Union and Swiss individuals with Privacy Shield inquiries or complaints should first contact us at privacy@honorlock.com with the subject line "**Privacy Shield**."

Honorlock has further committed to refer unresolved privacy complaints under the Privacy Shield Principles to an independent dispute resolution mechanism, the BBB EU PRIVACY SHIELD. If you do not receive timely acknowledgment of your complaint, or if your complaint is not satisfactorily addressed, please visit www.bbb.org/EU-privacy-shield/for-eu-consumers for more information and to file a complaint. This service is provided free of charge to you.

If your Privacy Shield complaint cannot be resolved through the above channels, under certain conditions, you may invoke binding arbitration for some residual claims not resolved by other redress mechanisms. See Privacy Shield Annex 1 at https://www.privacyshield.gov/article?id=ANNEX-I-introduction.

Onward Transfer to Third Parties under the Privacy Shield*:* Like many businesses, we hire other companies to perform certain business-related services. We may disclose personal information to certain types of third party companies but only to the extent needed to enable them to provide such services. The types of companies that may receive personal information and their functions are: hosting and storage services, relational databases and other storage providers (e.g., S3), proctoring processors, customer support tools, and analytics and marketing providers. All such third parties function as our agents, performing services at our instruction and on our behalf pursuant to contracts which require they provide at least the same level of privacy protection as is required by this Privacy Policy and implemented by Honorlock. We may also share your personal information with any of our parent companies, subsidiaries, affiliates, or other companies under common control with us for the purposes described in this Privacy Policy.

In certain situations, we may be required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements. We may also disclose personal data to other third parties when compelled to do so by government authorities or required by law or regulation including, but not limited to, in response to court orders and subpoenas.

Our accountability for personal data that we receive under the Privacy Shield and subsequently transfer to a third party is described in the Privacy Shield Principles. In particular, we remain responsible and liable under the Privacy Shield Principles if third-party agents that we engage to process the personal data on our behalf do so in a manner inconsistent with the Principles, unless we prove that we are not responsible for the event giving rise to the damage.

***Opt-In and Opt-Out under the Privacy Shield*:** We provide individuals with the opportunity to opt-out before we share your personal data with third parties other than our agents, or before we use it for a purpose that is materially different from which it was originally collected or subsequently authorized. To request to limit the disclosure of such personal data, please submit a written request to privacy@honorlock.com with the subject line, "**Privacy Shield**."

We will not disclose your sensitive personal information to any third party without first obtaining your opt-in consent, and shall also obtain your opt-in consent before we use sensitive data for a purpose other than which it was originally collected or subsequently authorized, unless an exception applies pursuant to the "Sensitive Data" Privacy Shield Supplemental Principal. In each instance, please allow us a reasonable time to process your response.

Where we act as a processor, we may pass on your request pursuant to this section to our customer (the controller).

Your Privacy Shield Rights: Pursuant to the Privacy Shield Frameworks, EEA, Swiss, and United Kingdom individuals have the right to obtain our confirmation of whether we maintain personal information relating to you in the United States. Upon request to privacy@honorlock.com with the subject line "**Privacy Shield**," we will provide you with confirmation as to whether we are processing your personal data pursuant to the Privacy Shield, and will communicate such data to you within a reasonable time. You have the right to correct, amend, or delete the personal data processed pursuant to the Privacy Shield where it is inaccurate or has been processed in violation of the Privacy Shield Principles. We may require payment of a non-excessive fee to defray our expenses in this regard. Please allow us a reasonable time to respond to your inquiries and requests.

Where we act as a processor, we may pass on your request pursuant to this section to our customer (the controller).

Retention of Personal Information under the Privacy Shield: We will retain the personal information processed pursuant to the Privacy Shield in a form that identifies you pursuant to our data retention periods in ***Retention*** above or as subsequently authorized. We may continue processing such personal information for longer periods, but only for the time and to the extent such processing reasonably serves the purposes of archiving in the public interest, journalism, literature and art, scientific or historical research and statistical analysis, and subject to the protection of our privacy disclosures. After such time periods have expired, we may either delete your personal information or retain it in a form such that it does not identify you personally.

How We Protect Your Personal Information under the Privacy Shield: Honorlock takes very seriously the security and privacy of the personal information that it collects pursuant to the

Privacy Shield. Accordingly, we will implement reasonable and appropriate security measures to protect your personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into account the risks involved in processing and the nature of such data, and comply with applicable laws and regulations.