Data Processing Agreement

This Data Processing Agreement ("DPA") is incorporated into the Agreement for all purposes to reflect the Parties' agreement related to the Processing of Personal Data.

1. Definitions

Capitalized terms not otherwise defined in this Addendum have the meaning given to them in the Agreement.

1.1 In this Addendum, the following terms have the meanings set out below:

1.1.1 "**Data Protection Laws**" means any and all applicable laws, rules, regulations, decrees, orders, or regulatory guidance relating to data security, data protection and/or privacy, in any jurisdiction, including but not limited to the EU General Data Protection Regulation, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (the "GDPR").

1.1.2 **"Customer Personal Data**" means, collectively, Customer Employee Personal Data and Customer Subscriber Personal Data.

1.1.3 "**Controller**" means the entity that determines the purpose and means of the processing of Customer Personal Data.

1.1.4 "**Customer Employee Personal Data**" means Personal Data relating to employees of Customer.

1.1.5 "**Customer Subscriber Personal Data**" means Personal Data relating to a Customer Subscriber.

1.1.6 "**Customer Subscriber**" means a Data Subject who purchases products or services from Customer.

1.1.7 "**Data Subject**" means an identified or identifiable person to whom Personal Data relates.

1.1.8 "**Data Subject Request**" means a request from an Data Subject seeking to exercise a right related to their Personal Data, either pursuant to Data Protection Laws or Customer's privacy policy (including requests to exercise any right of access, deletion, correction, object to processing, or restriction of processing).

1.1.9 "**Personal Data**" means any and all any information relating to an identified or identifiable natural person.

1.1.10 "**Processor**" means the entity that processes Customer Personal Data on Controller's behalf.

1.1.11 "**Subprocessor**" means any and all persons or entities (excluding an employee of Ory) appointed by or on behalf of Ory to process Personal Data on behalf of the Customer in connection with the Agreement.

2. Roles

2.1 The Parties acknowledge that Ory may collect and Process Customer Subscriber Personal Data when a Customer Subscriber uses a platform offered by Customer that has integrated a Product offered by

Ory. With regard to the Processing of Customer Subscriber Personal Data by Ory, Customer shall act as a Controller and Ory shall act as a Processor.

2.2 The Parties further acknowledge that Ory may collect and Process Customer Employee Personal Data when Data Subjects employed by Customer access the Website or other platforms offered by Ory in connection with the duties of their employment. With regard to the Processing of Customer Employee Personal Data by Ory, Ory shall act as a Controller.

3. Customer's Obligations

3.1 Customer shall ensure that Customer Subscribers receive a privacy notice that accurately reflects Customer's practices with regard to the Processing of Customer Subscriber Personal Data, including any and all practices that Customer does or will instruct Ory to carry out on Customer's behalf. Customer represents that the privacy notice includes, and will continue throughout the term of the Agreement to include, all information and disclosures required by Data Protection Laws. To the extent required by Data Protection Laws, Customer is responsible for obtaining any and all necessary Customer Subscriber consents with respect to Ory's Processing on behalf of Customer of Customer Subscriber Personal Data. Customer represents and warrants that it has complied and will continue to comply with Data Protection Laws in respect of its Processing of Personal Information and the Processing instructions it issues to Ory.

4. Processing of Customer Personal Data by Ory

4.1 Ory shall comply with all Data Protection Laws in the Processing of Customer Subscriber Data.

4.2 Ory shall ensure that (a) any access to Customer Personal Data is limited to those parties (including its personnel, agents, and Subprocessors) performing services in accordance with the Agreement and (b) any personnel who may have access to the Customer Personal Data have a need to know the relevant Customer Personal Data and are subject to legally binding obligations to keep the Customer Personal Data confidential.

4.3 Ory shall implement appropriate technical and organisational measures (Appendix 1) to ensure a level of security for Customer Personal Data appropriate to the risk, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing of the Customer Personal Data as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

5. Additional Requirements for Processing of Customer Subscriber Personal Data by Ory

5.1 **Compliance with Controller instructions**. With respect to Customer Subscriber Personal Data, Ory shall:

5.1.1 only process Customer Subscriber Personal Data pursuant to Customer's instructions as set forth in this Agreement or as otherwise updated by Customer in writing from time to time;

5.1.2 promptly notify Customer in writing if Ory becomes aware of or believes that any processing instruction from Customer violates Data Protection Laws, or if Ory is unable to comply with Data Protection Laws or its obligations under this Addendum;

5.1.3 limit the processing of Customer Personal Data to the processing that is reasonably necessary and proportionate to provide the Products described in the Agreement.

5.2 **Subprocessing.** Customer hereby grants general written authorization to Ory to appoint Subprocessors (Appendix 2) to perform specific Processing activities on its behalf. Customer approves those Subprocessors Ory has engaged as of the date of this Addendum. Ory shall provide written notification to Customer regarding the replacement or addition of Subprocessors. Customer may object in writing to any additional or replacement Subprocessor on reasonable data protection grounds within thirty (30) business days after receipt of the notice. If Customer objects, and Customer and Ory cannot agree on a commercially reasonable, either party has the right to terminate the Agreement with respect to only those Products which cannot be provided by Ory without the use of the objected to Subprocessor. Ory further agrees that it shall:

1.1.1 enter into a written agreement with each Subprocessor imposing data protection obligations no less protective of Customer Subscriber Personal Data as those imposed on Ory under this Addendum and that meet the requirements of Data Protection Laws;

1.1.2 disclose to Subprocessors only the minimum amount of Customer Personal Data necessary to perform the Services.

1.2 **Data Subject Requests.** Ory shall implement reasonable technical and administrative measures to enable Ory and its agents and employees to promptly assist Customer with any and all Data Subject Rights Requests related to Customer Subscriber Personal Data Processed by Ory. In the event that Ory receives a request, inquiry, notice, or complaint from an Data Subject relating to Customer Subscriber Personal Data (including requests to exercise any right of access, deletion, correction, objection to processing, or restriction of processing), Ory may respond to the Data Subject solely to direct the Data Subject to submit their request to Customer, unless otherwise required by Data Protection Laws.

1.3 **Third-Party Demands and Government Access.** If Ory (or any Subprocessor) receives a request to retain, disclose, or otherwise process Customer Subscriber Personal Data from any third party, including any government authority ("**Third-Party Request**"), Ory shall, to the extent legally permitted, immediately notify Customer in writing and provide all relevant details of the Third-Party Request. In the event Ory is prohibited from providing the foregoing notice to Customer, Ory shall use best efforts to obtain a waiver of the prohibition to enable Ory to communicate as much information to Customer as possible, as soon as possible. Ory shall challenge a Third-Party Request if, after careful assessment, it determines that there are reasonable grounds to conclude that the request is unlawful. To the extent Ory is legally required to comply with any Third-Party Request, Ory shall disclose only the portion of Customer Personal Data that is required to be disclosed and use reasonable efforts to obtain assurances that such Customer Personal Data will be treated confidentially.

1.4 **Data Protection Impact Assessment and Prior Consultation**. Ory shall assist Customer in meeting Customer's obligations in relation to data protection impact assessments and prior consultations with any government authority by fully cooperating with all requests from Customer for information about Ory's and its Subprocessors' processing activities and data protection practices, taking into account the nature of processing and the information available to Ory.

1.5 **Deletion or Return of Customer Personal Data**. Ory shall delete Customer Subscriber Personal Data in the ordinary course of business when no longer necessary to perform Services under the Agreement, pursuant to the instructions of Customer. After the termination or expiration date of the Agreement, Ory shall provide Customer with a copy of any and all remaining Customer Personal Data and then shall delete such Customer Personal Data from Ory's systems, unless retention is required by applicable law.

1.6 **Survival**. The terms of this Section 5 shall apply for as long as Ory maintains Customer Subscriber Personal Data.

2. International Data Transfers

2.1 If Ory transfer Customer Personal Data for Processing outside the U.S., E.U., or U.K. (**"Restricted Transfers"**), Ory shall establish an appropriate transfer mechanism with the recipient of such Customer Personal Data, as required by Data Protection Laws.

Appendix 1 to the DPA: Technical and Organizational Measures Designed to Ensure the Security of the Customer Personal Data

Ory uses the following technical and organisational measures to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons:

Topic	Practices
Organization of Information Security	Security Ownership Ory has appointed an individual to the role of a security officer for coordinating and monitoring Ory's security policies and procedures. Security Roles and Responsibilities Ory personnel with access to the Customer Personal Data are subject to confidentiality obligations. Risk Management Program Ory has established a formal Risk Management Program and maintains a Risk Register. Ory performs regular risk assessments and quarterly risk reviews with management. Vendor Management Ory has a vendor risk assessment process that is designed to implement vendor contract clauses and additional data protection agreements with vendors. Security Assessments Ory conducts internal and external security assessments on a regular basis and such security assessments are designed to ensure the effectiveness of security and compliance controls. These assessments may include audits, penetration testing and independent reviews of security professionals.
Asset Management	Asset Inventory Ory maintains an inventory of all asset on which the Customer Personal Data is stored. Access to such data is restricted to Ory personnel authorized to have such access. Asset Handling ● Ory classifies the Customer Personal Data to help identify it and to allow for access to it to be appropriately restricted. ● Ory communicates and enforces employee responsibility and accountability for data protection up to and including cause for termination. ● Ory personnel must obtain Ory's authorization prior to processing the Customer Personal Data outside of Ory's environments.
Human Resource Security	Security Training Ory requires all new hires to complete security and privacy awareness training as part of initial on-boarding. Participation in annual training is required for all employees to provide a baseline for security and privacy basics.
Physical and Environmental Security	Physical Access to Facilities Ory is not operating any data centers in its own facilities. Ory uses commercially reasonable efforts to ensure that physical access to the data centers of the cloud providers

Topic	Practices
	is secured in accordance with industry standards through a multi-layered approach and is regularly checked through Ory's Vendor Risk Assessment. Protection from Disruptions Ory uses commercially reasonable efforts to ensure that Ory's cloud providers use a variety of industry standards and best practices designed to protect against outages or failures of their own data centers. Ory Network uses redundancy throughout its setup, which is designed to eliminate single points of failure to ensure high availability.
Communications and Operations Management	Operational Policy Ory maintains security documents designed to describe its security measures and the relevant procedures and responsibilities of its personnel who have access to the Customer Personal Data. Security & Privacy by Design ● Ory follows a Security Development Lifecycle (SDL) program consisting of a set of practices that are designed to support security assurance and compliance requirements. The SDL helps developers build more secure software by reducing the number and severity of vulnerabilities in software, while reducing development cost. ● Ory follows the Privacy by Design principles with regular Privacy Impact Assessments. Change Management & Configuration Management ● Ory Network's configuration is managed in a version control system. Any change to its configuration is captured in an audit log. Changes to the production and staging environments require a strict approval process involving two or more employees. ● Changes applied to an Ory Network environment can be rolled back by reverting the change set in question. ● Promoting changes to the production environment requires the approval of the Change Advisory Board. Anti-Malware Management / Malicious Software / Protective Technology ● Ory validates that commercially reasonable Anti-Virus & Anti-Malware software is running on Ory-owned notebooks and devices. ● The Ory Network locks down network communication to suppress non-standard communication in the cluster (Network Policies) ● The Ory Network uses WAF solutions to actively prevent remote exploitation of vulnerabilities Vulnerability & Patch Management ● Ory scans its own components during build time for known vulnerabilities and reports on any present vulnerability. ● Ory scans all components (including used third party components) running in the Ory Network environments at runtime at least once a day and reports any

Topic	Practices
	vulnerabilities ● Ory reviews the vulnerability management of the third party on a regular basis. ● Ory utilizes a highly automated patch management tool that implements CI/CD pipelines and uses embedded approval workflows to apply changes to different environments. Data Security in transit and at-rest ● The Ory Network encrypts data transferred to/from Ory Network using TLS 1.2 or higher ● The Ory Network encrypts the Customer Personal Data at-rest using industry standard AES-256 encryption.
Access Control	Access Policy Ory maintains a record of security privileges of individuals having access to the Customer Personal Data. Access Authorization ● Ory maintains and updates a record of personnel authorized to access Ory's systems that contain the Customer Personal Data. ● Ory identifies those personnel who may grant, alter or cancel authorized access to the Customer Personal Data. ● Ory has designed processes designed to ensure that where more than one individual has access to systems containing the Customer Personal Data, the individuals have separate identifiers/log-ins where technically and architecturally feasible, and commercially reasonable. Least Privilege ● Technical support personnel are only permitted to have access to the Customer Personal Data when needed to perform their job functions. ● Ory restricts access to the Customer Personal Data to only those individuals who require such access to perform their job function. Ory employees are only granted access to production systems based on their role within the organization. Integrity and Confidentiality ● Ory instructs Ory personnel to disable administrative sessions when computers are left unattended. ● Ory stores passwords such that they are encrypted or unintelligible while they are in force. Authentication ● Ory uses industry standard practices to identify and authenticate users who attempt to access information systems. ● Access to third party systems is secured using multi-factor authentication ● Ory ensures that de-activated or expired employee identifiers are not granted to

Topic	Practices
	other individuals. ● Ory monitors, or may (in Ory's sole discretion) enable the Customer to monitor, repeated attempts to gain access to the information system using an invalid password. ● Ory maintains industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed. ● Ory uses industry standard password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage. Network Design Ory has implemented controls designed to ensure no systems storing the Customer Personal Data are part of the same logical network used for Ory business operations.
Information Security Incident Management	Incident Response Process ● Ory maintains a record of security incidents with a description of the incidents, the time period, the consequences of the breach, the name of the reporter, and to whom the incident was reported, and details regarding the handling of the incident. ● In the event that Ory Security confirms or reasonably suspects that an Ory customer is affected by a data breach, Ory notifies the customer within a commercially reasonable period in accordance with applicable law ● Ory tracks, or may (in Ory's sole discretion) enable the Customer to track, disclosures of the Customer Personal Data, including what data has been disclosed, to whom, and at what time. Service Monitoring Ory employs a wide range of continuous monitoring solutions designed for preventing, detecting, and mitigating attacks to the site.
Business Continuity Management	● On an ongoing basis, but in no case less frequently than once a day, Ory maintains a backup of the Customer Personal Data from which the Customer Personal Data can be recovered. ● Ory has implemented procedures governing access to copies of the Customer Personal Data. ● Ory maintains emergency and contingency plans for the facilities in which Ory information systems that process the Customer Personal Data are located. ● Ory's redundant storage and its procedures for recovering data are designed to attempt to reconstruct the Customer Personal Data in its original or last-replicated state from before the time it was lost or destroyed. ● Ory performs testing of the disaster recovery capabilities on a regular basis.

Appendix 2 to the DPA: List of Subprocessors

Ory currently uses the following Subprocessors to support its cloud environment and business operations. The Customer Personal Data processed by Subprocessors is processed for the purposes and duration of the relevant services agreement between Ory and that Subprocessor.

Name and Address of the Subprocessor*	Purpose of the Processing/Service Provided*	Countries where the Customer Personal Data will be Processed*
CloudFlare, Inc. **101 Townsend St,** **San Francisco, CA 94107** **USA**	DDOS Protection, Firewall, DNS, TLS, Rate-Limiting, CDN and Edge Worker Services	Countries: USA, United Kingdom, Singapore, Australia, Germany, Portugal, France, Japan, Canada, Netherlands, Dubai. Subprocessors: https://www.cloudflare.com/en-gb/gdpr/subprocessors/
Cockroach Labs, Inc. **125 W. 25th Street, 11th Floor** **New York, NY 10001** **USA**	Database Services	Countries: USA, Belgium, Germany Subprocessors: https://www.cockroachlabs.com/cloud-terms-and-conditions/data-processing-addendum/cockroach-labs-sub-processors/
GitHub, Inc **88 Colin P Kelly Junior Street** **San Francisco, CA 94107** **USA**	Customer support	Countries: USA Subprocessors: https://docs.github.com/en/github/site-policy/github-subprocessors-and-cookies
Google LLC **1600 Amphitheatre Parkway** **Mountain View, CA 94043** **USA**	Cloud Service Provider: Storage, Compute, Managed Kubernetes, Network and Firewall functionality.	Countries: USA, European Economic Area Subprocessors: https://cloud.google.com/terms/subprocessors
HubSpot, Inc. **25 First Street, 2nd Floor** **Cambridge, MA 02141** **USA**	CRM Solution	Countries: USA Subprocessors: https://legal.hubspot.com/dpa
Mailgun Technologies **112 E. Pecan Street #1135,** **San Antonio, Texas, 78205** **USA**	Transactional mail services provider	Countries: USA, France, Sweden Subprocessors: https://www.mailgun.com/dpa/
Slack Technologies, LLC **500 Howard Street** **San Francisco, CA 94105** **USA**	Customer support communications	Countries: USA Subprocessors: https://slack.com/terms-of-service/slack-subprocessors

Name and Address of the Subprocessor*	Purpose of the Processing/Service Provided*	Countries where the Customer Personal Data will be Processed*
Stripe, Inc. **354 Oyster Point Boulevard** **South San Francisco, CA, 94080** **USA**	Credit card payment processing. Customers submit information directly to Stripe through Stripe's API. Ory does not handle credit card information.	Countries: USA Subprocessors: https://stripe.com/en-gb-de/service-providers/legal#list-of-affiliates
PostHog Inc **2261 Market Street #4008** **San Francisco** **CA 94114** **USA**	Product Analytics using pseudonymist data	Countries: Germany Subprocessors: https://docs.google.com/document/d/1xfpP1SCFoI1qSKM6rEt9VqRLRUEXiKj9_0Tvv2mP928/edit
Functional Software, Inc., t/a 'Sentry' **45 Fremont Street, 8th Floor** **San Francisco** **CA 94105** **USD**	Application monitoring and error tracking	Countries: USA Subprocessors: https://sentry.io/legal/dpa/#list-of-subprocessors-1
Zendesk, Inc. **989 Market St** **San Francisco, CA 94103**	Customer support ticketing and communications	Countries: USA Subprocessors: https://support.zendesk.com/hc/en-us/articles/4408883061530-Sub-processor-Policy