Functional Software, Inc.

Data Processing Addendum

(Revision May 2024)

Legal Name of Customer Entity:	The Hack Foundation (ATC24 Controllers) *(Insert name of Customer entity)*

This Data Processing Addendum (this "DPA") is entered into and effective as of the last date of signature below by and between Functional Software, Inc. d/b/a Sentry ("Sentry", "we", or "us") and the party named above ("Customer", or "you").

You have entered into one or more agreements with us (each, as amended from time to time, an "Agreement") governing the provision of our real-time error tracking, crash reporting, application monitoring, visibility and software test coverage reporting services more fully described at https://sentry.io and https://about.codecov.io (as applicable, the "Service"). This DPA will amend the terms of the Agreement to reflect the parties' rights and responsibilities with respect to the processing and security of Customer Data (as defined below) under the Agreement. If you are accepting this DPA in your capacity as an employee, consultant or agent of Customer, you represent that you are an employee, consultant or agent of Customer, and that you have the authority to bind Customer to this DPA.

Any capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement.

1. Definitions. The following definitions apply to this DPA:

"CCPA" means the California Consumer Privacy Act, as amended by the California Privacy Rights Act, and any binding regulations promulgated thereunder.

"Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of processing of Personal Data.

"Customer Data" means data you submit to, store on or send to us via the Service.

"Data Incident" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to, Personal Data on systems that are managed and controlled by Sentry. Data Incidents will not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including, without limitation, pings, port scans, denial of service attacks, network attacks on firewall or networked systems or unsuccessful login attempts.

"Data Privacy Framework" means (as applicable) the EU-U.S. Data Privacy Framework, the Swiss-U.S. Data Privacy Framework and the UK Extension to the EU-U.S. Data Privacy Framework self-certification programs operated by the U.S. Department of Commerce, and their respective successors.

"Data Privacy Framework Principles" means the Principles and Supplemental Principles contained in the relevant Data Privacy Framework, as may be amended, superseded or replaced.

"data subject" means the identified or identifiable natural person to whom Personal Data relates.

"Europe" means, for the purposes of this DPA, the member states of the European Economic Area, Switzerland, and the United Kingdom.

"European Data Protection Legislation" means the data protection and privacy laws and regulations enacted in Europe and applicable to the Personal Data in question, including as applicable: (i) the GDPR; (ii) the Swiss Federal Act on Data Protection of 2020 and its Ordinance ("Swiss FADP"); and (iii) in respect of the United Kingdom, the GDPR as it forms part of UK law by virtue of Section 3 of the European Union (Withdrawal) Act 2018 ("UK GDPR") and the Data Protection Act 2018; in each case as may be amended, superseded or replaced from time to time.

“GDPR” means Regulation (EU) 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.

“Notification Email Address” means the email address that you designate to receive notifications when you create an account to use the Service. You agree that you are solely responsible for ensuring that your Notification Email Address is current and valid at all times.

“Personal Data” means information about an identified or identifiable natural person or which otherwise constitutes “personal data”, “personal information”, “personally identifiable information” or similar terms as defined in Privacy Laws that is contained within Customer Data.

“Privacy Laws” means: (i) European Data Protection Legislation and (ii) U.S. Data Protection Legislation.

“processing” (and “process”) means any operation or set of operations that is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

“Processor” means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller.

“Standard Contractual Clauses” or “SCCs” means the standard contractual clauses as approved by the European Commission pursuant to its decision 2021/914 of 4 June 2021.

“Subprocessor” means a third party that we use to process Customer Data in order to provide parts of the Service and/or related technical support. For the avoidance of doubt, the term Subprocessor may include Sentry affiliates or other third parties but does not include Sentry employees or contractors.

“Term” means the term of the Agreement.

“UK Addendum” means the International Data Transfer Addendum (version B1.0) issued by the Information Commissioner's Office under s.119(A) of the UK Data Protection Act 2018, as may be amended, superseded or replaced from time to time.

“U.S. Data Protection Legislation” means the data protection and privacy laws and regulations enacted in the United States and applicable to the Personal Data in question, including as applicable the CCPA, as may be amended, superseded or replaced from time to time.

2. **Data Processing**.

2.1 Roles and Regulatory Compliance; Authorization.

2.1.1 *Scope of this DPA*. This DPA applies where and only to the extent Sentry processes Personal Data as a Processor for the purposes of Privacy Laws.

2.1.2 *Roles and Responsibilities*. The parties acknowledge and agree that: (i) Sentry will process the Personal Data as described in Schedule 1; (ii) Sentry is a Processor of Personal Data and Customer is the Controller (or a Processor acting on behalf of a third-party Controller); and (iii) each of us will comply with our obligations under Privacy Laws with respect to the processing of Personal Data.

2.1.3 *Authorization by Third Party Controller*. If you are a Processor of Personal Data acting on behalf of a third-party Controller: (i) you warrant to us that your instructions and actions with respect to that Personal Data, including your appointment of Sentry as another Processor, have been authorized by the relevant Controller; and (ii) you will serve as our sole point of contact and where we would otherwise be required (including for the purposes of the Standard Contractual Clauses) to provide information, assistance or cooperation to or seek authorization from any such third-party Controllers, we may provide such information, assistance or cooperation to or seek such authorization from you.

2.2 Customer responsibilities.

2.2.1 *Customer Authorization*. Sentry shall process Personal Data in accordance with Customer's documented lawful instructions. By entering into this DPA, you hereby authorize and instruct us to process Personal Data: (i) to provide the Service, and related technical support; (ii) as otherwise permitted or required by your use of the Service or your requests for technical support; (iii) as otherwise permitted or required by the Agreement, including this DPA; and (iv) as further documented in any other written instructions that are agreed by the parties. We will not process Personal Data for any other purpose, unless required to do so by applicable law or regulation. The parties agree that the Agreement (including this DPA), and your use of the Service in accordance with the Agreement, set out your complete and final processing instructions and any processing outside the scope of these instructions (if any) shall require prior written agreement between the parties. Customer shall ensure its instructions are lawful and that the processing of Personal Data in accordance with such instructions will not violate Privacy Laws. Notwithstanding the foregoing, if you are a Processor of Personal Data acting on behalf of a third-party Controller then where legally required we are entitled to follow the instructions of such third-party Controller with respect to their Personal Data.

2.2.2 *Prohibition on Sensitive Data*. You will not submit, store, or send any sensitive personal information or special categories of personal data (collectively, "Sensitive Data") to us for processing, and you will not permit nor authorize any of your employees, agents, contractors or data subjects to submit, store or send any Sensitive Data to us for processing. You acknowledge that we do not request or require Sensitive Data as part of providing the Service to you, that we do not wish to receive or store Sensitive Data, and that our obligations in this DPA will not apply with respect to Sensitive Data. The terms "sensitive personal information" and "special categories of personal data" have the meanings given in Privacy Laws.

3. Deletion.

3.1 Deletion During Term. We will enable you to delete Personal Data during the Term in a manner that is consistent with the functionality of the Service. If you use the Service to delete any Personal Data in a manner that would prevent you from recovering Personal Data at a future time, you agree that this will constitute an instruction to us to delete Personal Data from our systems in accordance with our standard processes and applicable law. We will comply with this instruction as soon as reasonably practicable, but in all events in accordance with applicable law.

3.2 Deletion When Term Expires. When the Term expires, we will destroy any Personal Data in our possession or control. This requirement will not apply to the extent that we are required by applicable law to retain some or all of the Personal Data, in which event we will isolate and protect the Personal Data from further processing and delete in accordance with Sentry's deletion practices, except to the extent required by law. You acknowledge that you will be responsible for exporting, before the Term expires, any Personal Data you want to retain after the Term expires.

4. Data Security.

4.1 Security Measures. We will implement and maintain appropriate technical and organizational measures to protect Personal Data against Data Incidents and to preserve the security and confidentiality of Personal Data, as described in Schedule 2 (collectively, the "Security Measures"). Sentry shall ensure that any person who is authorized by Sentry to process Personal Data shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty). Customer acknowledges that Security Measures are subject to technical progress and development and that accordingly we may update or modify the Security Measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Service.

4.2 Data Incidents. Upon becoming aware of a Data Incident, we will notify you promptly and without undue delay, and will take reasonable steps to minimize harm and secure Personal Data. Any notifications that we send you pursuant to this Section 4.2 will be sent to your Notification Email Address and will describe, to the extent possible and known to Sentry, the details of the Data Incident, the steps we have taken to mitigate the potential risks, and any suggestions we have for you to minimize the impact of the Data Incident. We will not assess the contents of any Personal Data in order to identify information that may be subject to specific legal requirements. You are solely responsible for complying with any incident notification laws that may apply to you, and to fulfilling any third-party notification obligations related to any Data Incident. Our notification of or response to a Data Incident under this Section will not constitute an acknowledgement of fault or liability with respect to the Data Incident.

4.3 Your Security Responsibilities. You agree that, without prejudice to our obligations under Sections 4.1 or 4.2 above, you are solely responsible for your use of the Service, including making appropriate use of the Service to ensure a level of security appropriate to the risk in relation to Customer Data, securing any account authentication credentials, systems and devices you use to access the Service, and backing up your Customer Data. You understand and agree that we have no obligation to protect Customer Data that you elect to store or transfer outside of our or our Subprocessors' systems (e.g., offline or on-premise storage). You are solely responsible for evaluating whether the Service and our commitments under this Section 4 meet your needs, including with respect to your compliance with any of your security obligations under Privacy Laws, as applicable.

4.4 Audit Rights.

4.4.1 *Audit Reports.* You acknowledge that Sentry is regularly audited against various information security standards by independent third-party auditors and internal auditors, respectively. Upon request, we shall supply (on a confidential basis) a summary copy of our audit reports, so that you can verify our compliance with the audit standards against which it has been assessed, and this DPA. Further, we will provide written responses (on a confidential basis) to all reasonable requests for information necessary to confirm our compliance with this DPA, provided that you will not exercise this right more than once per calendar year.

4.4.2 *Independent Audits.* While it is the parties' intention to rely ordinarily on the provision of the above audit reports to verify our compliance with this DPA, we will allow an internationally-recognized independent auditor that you select to conduct audits to verify our compliance with our obligations under this DPA. You must send any requests for audits under this Section 4.4.2 to legal@sentry.io. Following our receipt of your request, the parties will discuss and agree in advance on the reasonable start date, scope, duration and security and confidentiality controls applicable to the audit. You will be responsible for any costs associated with the audit. You agree not to exercise your audit rights under this Section 4.4.2 more than once in any twelve (12) calendar month period, except (i) if and when required by a competent data protection authority; or (ii) an audit is necessary due to a Data Incident. You agree that (to the extent applicable), you shall exercise any audit rights under Privacy Laws and the Standard Contractual Clauses by instructing us to comply with the measures described in this Section 4.4.

5. Data Subject Rights; Data Export.

5.1 Access; Rectification; Restricted Processing; Portability. You acknowledge that the Service may, depending on the functionality of the Service, enable you to: (i) access the Customer Data; (ii) rectify inaccurate Customer Data; (iii) restrict the processing of Customer Data; (iv) delete Customer Data; and (v) export Customer Data.

5.2 Cooperation; Data Subjects' Rights. To the extent that you cannot access the relevant Personal Data within the Service, we will provide you, at your expense, with all reasonable and timely assistance to enable you to respond to: (i) requests from data subjects who wish to exercise any of their rights under applicable Privacy Laws; and (ii) any other correspondence, enquiry or complaint received from a data subject, government authority or other third party in connection with the processing of the Customer Data. In the event that any such request, correspondence, enquiry or complaint is made directly to us, we will promptly inform you of it, and provide you with as much detail as reasonably possible.

6. Data Transfers.

6.1 Data Storage and Processing Facilities. You agree that we may, subject to Section 6.2, store and process Customer Data in the United States and any other country in which we or our Subprocessors maintain data processing operations. Sentry shall ensure that such transfers are made in compliance with applicable Privacy Laws and this DPA.

6.2 Transfers of Data out of Europe. If the storage and processing of Personal Data as described in Section 6.1 involves a transfer of Personal Data that is subject to European Data Protection Legislation ("European Personal Data") to Sentry outside of Europe, then Sentry will comply with Schedule 3 (Cross-Border Transfer Mechanisms).

7. Subprocessors.

7.1 Consent to Engagement. You authorize us to engage third parties as Subprocessors. Whenever we engage a Subprocessor, we will enter into a contract with that Subprocessor which imposes data protection terms that require the Subprocessor to protect Personal Data to an equivalent standard required under this DPA, and we shall remain responsible for the Subprocessor's compliance with the obligations of this DPA and for any acts or omissions of the Subprocessor that cause us to breach any of our obligations under this DPA.

7.2 List of Subprocessors. A list of our current Subprocessors is available at https://sentry.io/legal/subprocessors/ or such other website as Sentry may designate ("Subprocessor Page"). We may update the Subprocessor Page from time to time to reflect any changes in Subprocessors. We will provide thirty (30) days' prior written notice to you via email or other means specified on the Subprocessor Page. During this period you will have the opportunity to object as described in Section 7.3 below.

7.3 Objections; Sole Remedy. You have the right to object to the appointment or replacement of a Subprocessor prior to its appointment or replacement on reasonable grounds that the Subprocessor does not or cannot comply with the requirements set forth in this DPA (each, an "Objection"). If we do not remedy or provide a reasonable workaround for your Objection within a reasonable time, you may, as your sole remedy and our sole liability for your Objection, terminate the Agreement for your convenience, and without further liability to either party.

7.4 Disclosure of Subprocessor agreements. You agree that by complying with this Section 7, we fulfil our obligations under Clause 9(a) and (b) of the Standard Contractual Clauses. You further acknowledge that, for the purposes of Clause 9(c) of the Standard Contractual Clauses, we may be restricted from disclosing Subprocessor agreements to you (or the relevant third-party Controller) due to confidentiality restrictions. Notwithstanding this, we shall use reasonable efforts to require Subprocessors to permit us to disclose Subprocessor agreements to you and, in any event, will provide (upon request and on a confidential basis) all information we reasonably can in connection with such Subprocessor agreement.

8. Data Protection Impact Assessment. We will provide you with reasonable and timely assistance as you may require in order to conduct a data protection impact or similar risk assessment related to your use of the Service and, if required by Privacy Laws, consult with the relevant government authority.

9. Jurisdiction Specific Terms. The terms specified in Schedule 4 with respect to the listed jurisdictions will apply in addition to the terms of this DPA.

10. Miscellaneous. With the exception of the third-party beneficiary rights granted (where applicable) under the Standard Contractual Clauses, there are no third-party beneficiaries to this DPA. Except as expressly provided herein, nothing in this DPA will be deemed to waive or modify any of the provisions of the Agreement, which otherwise remains in full force and effect. Specifically, nothing in this DPA will affect any of the terms of the Agreement relating to Sentry's limitations of liability, which will remain in full force and effect. Notwithstanding the foregoing, in no event shall either party exclude or limit its liability with respect to any data subject's rights under European Data Protection Legislation or the Standard Contractual Clauses. If you have entered into more than one Agreement with us, this DPA will amend each of the Agreements separately. In the event of a conflict or inconsistency between the terms of this DPA and the terms of the Agreement, the terms of this DPA will control. This DPA amends and supersedes any prior data processing addendum or similar agreement regarding its subject matter.

11. Change in Privacy Laws. Notwithstanding anything to the contrary in the Agreement (including this DPA), in the event of a change in Privacy Laws or a determination or order by a government authority or competent court affecting this DPA or the lawfulness of any processing activities under this DPA, we reserve the right to make any amendments to this DPA as are reasonably necessary to ensure continued compliance with Privacy Laws or compliance with any such orders.

IN WITNESS WHEREOF, the parties cause this DPA to be signed by their duly authorized representatives as set out below.

FUNCTIONAL SOFTWARE, INC. DBA SENTRY		CUSTOMER	
Signature:	DocuSigned by: Virginia Badenhope A6CC15DAFEE04C4...	Signature:	Signed by: Jose Moran Urena 597BB74A191644A...
Name:	Virginia Badenhope	Name:	Jose Moran Urena
Title:	General Counsel	Title:	Operations Manager
Date:	5/3/2025	Date:	5/3/2025

Schedule 1

Unless otherwise specified below, this schedule applies to both the Service further described at https://sentry.io (the "Sentry Service") and https://about.codecov.io (the "Codecov Service").

A. List of Parties

Data exporter(s):

Name: Customer (as defined in the DPA)

Address: Customer's address (as specified in the Agreement)

Contact person's name, position and contact details: Customer's contact details (as specified in the Agreement)

Role (controller/processor): Controller/processor

Data importer(s):

Name: Functional Software, Inc. d/b/a Sentry

Address: 45 Fremont Street, 8th Floor, San Francisco, CA 94105

Contact person's name, position and contact details: Virginia Badenhope, General Counsel, legal@sentry.io

Role (controller/processor): Processor

B. Data Processing Description

Subject Matter: Sentry's provision of the Service to Customer, and related technical support.

Purpose of the Processing: Sentry will process personal data submitted to, stored on, or sent via the Service for the purpose of providing the Service and related technical support in accordance with this DPA.

Sentry Service

Categories of Data Subjects: Data subjects who interact with the software, system or application that Customer has chosen to monitor using the Service, which may include Customer's users and customers, as determined by Customer in the configuration of the Service.

Categories of Personal Data: Personal data that is submitted to the Service by Customer, which may include IP address, email address and other types of identifiable data configured by Customer, subject to the restrictions in this DPA.

Codecov Service

Categories of Data Subjects: Data subjects who contribute code to or are otherwise project members of Customer's code repository that Customer has integrated with the Service, which may include Customer's employees and contractors.

Categories of Personal Data: Code repository username, email address (if made publicly available by the data subject in the code repository) and code repository ID from the code repository that Customer has chosen to integrate with the Service.

Sensitive Data: Customer determines and controls the personal data transferred to Sentry and is solely responsible for ensuring the legality of the categories of data it may choose to transfer to Sentry. This DPA includes an express prohibition on the transfer of special categories of personal data to Sentry.

Frequency of the Transfer: Continuous

Nature of the Processing: Sentry will perform the following basic processing activities: processing to provide the Service in accordance with the Agreement; processing to perform any steps necessary for the performance of the

Agreement; and processing to comply with other reasonable instructions provided by Customer (e.g. via email) that are consistent with the terms of the Agreement.

Period for which the personal data will be retained: Throughout the Term of the Agreement plus the period from expiry of the Term until deletion of Personal Data by Sentry in accordance with the Agreement.

C. Competent Supervisory Authority

The Irish Data Protection Commissioner.

Schedule 2

Security Measures

This Schedule 2 describes Security Measures, as applicable to each of the Service further described at https://sentry.io (the "Sentry Service") and https://about.codecov.io (the "Codecov Service").

Sentry Service

Security Measures for the Sentry Service include the technical and organizational measures set forth below and in the current version of the Sentry Service Security Policy available at https://sentry.io/security/.

Technical and Organizational Measures	Relevant Section(s) of Sentry Service Security Policy
Measures of pseudonymization and encryption of personal data	● Data Flow – Data into System ● Data Flow – Data through System ● Data Security and Privacy – Data Encryption ● Data Security and Privacy – PII Scrubbing
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	● Infrastructure and Network Security – Physical Access Control ● Infrastructure and Network Security – Logical Access Control ● Application Security – Multi-Factor Authentication ● Application Security – Single Sign-On ● Application Security – SAML 2.0 ● Application Security – REST API Authentication (API Key) ● Application Security – Audit Controls
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	● Infrastructure and Network Security – Intrusion Detection and Prevention ● Business Continuity and Disaster Recovery ● Corporate Security – Contingency Planning ● Corporate Security – Vulnerability Disclosure
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	● Infrastructure and Network Security – Penetration Testing ● Infrastructure and Network Security – Third-Party Audit ● Corporate Security – Risk Management ● Corporate Security – Security Policies
Measures for user identification and authorization	● Infrastructure and Network Security – Logical Access Control ● Application Security – Multi-Factor Authentication ● Application Security – Single Sign-On ● Application Security – SAML 2.0 ● Application Security – REST API Authentication (API Key) ● Application Security – Audit Controls
Measures for the protection of data during transmission	● Data Flow – Data Through System
Measures for the protection of data during storage	● Data Security and Privacy – Data Encryption
Measures for ensuring physical security of locations at which personal data are processed	● Infrastructure and Network Security – Physical Access Control
Measures for ensuring events logging	● Application Security – Audit Controls
Measures for ensuring system configuration, including default configuration	● Application Security – Secure Application Development (Application Development

Technical and Organizational Measures	**Relevant Section(s) of Sentry Service Security Policy**
	Lifecycle) ● Corporate Security – Risk Management ● Corporate Security – Security Policies
Measures for internal IT and IT security governance and management	● Security and Compliance ● Infrastructure and Network Security – Third-Party Audit ● Corporate Security – Risk Management
Measures for certification/assurance of processes and products	● Infrastructure and Network Security – Third-Party Audit ● Corporate Security – Risk Management
Measures for ensuring data minimization	● Data Security and Privacy – Data Retention ● Data Security and Privacy – Data Removal
Measures for ensuring data quality	● Data Flow – Data Through System ● Data Security and Privacy – Data Encryption ● Application Security – Audit Controls ● Sentry maintains an online form to allow data subjects to request a copy of their personal data, make changes to their personal data or request deletion of their personal data
Measures for ensuring limited data retention	● Data Security and Privacy – Data Retention ● Data Security and Privacy – Data Removal
Measures for ensuring accountability	● Corporate Security – Risk Management ● Corporate Security – Security Policies
Measures for allowing data portability and ensuring erasure	● Sentry maintains an online form to allow data subjects to request a copy of their personal data, make changes to their personal data or request deletion of their personal data
Measures and assurances regarding U.S. government surveillance ("Additional Safeguards")	● Sentry uses encryption both in transit and at rest. ● As of the date of this DPA, Sentry has not received any national security orders of the type described in Paragraphs 150-202 of the judgment in the EU Court of Justice Case C-311/18, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems. ● No court has found Sentry to be the type of entity eligible to receive process issued under FISA Section 702: (i) an "electronic communication service provider" within the meaning of 50 U.S.C § 1881(b)(4) or (ii) a member of any of the categories of entities described within that definition. ● Sentry shall not comply with any request under FISA for bulk surveillance, i.e., a surveillance demand whereby a targeted account identifier is not identified via a specific "targeted selector" (an identifier that is unique to the targeted endpoint of communications subject to the surveillance). ● Sentry shall use all available legal mechanisms to challenge any demands for data access through national security process that Sentry receives, as well as any non-disclosure provisions attached thereto.

Technical and Organizational Measures	Relevant Section(s) of Sentry Service Security Policy
	● Sentry shall take no action pursuant to U.S. Executive Order 12333. ● Sentry publishes a transparency report indicating the types of binding legal demands for the personal data it has received, including national security orders and directives, which shall encompass any process issued under FISA Section 702. ● Sentry will notify Customer if Sentry can no longer comply with the Standard Contractual Clauses or these Additional Safeguards, without being required to identify the specific provision with which it can no longer comply.

Codecov Service

Security Measures for the Codecov Service include the technical and organizational measures set forth below and in the current version of the Codecov Service Security Policy available at https://about.codecov.io/security/.

Technical and Organizational Measures	Relevant Section(s) of Codecov Service Security Policy (if applicable)
Measures of pseudonymization and encryption of personal data	Data is encrypted at rest. Data transfers are secured using Transport Layer Security (TLS) and industry-standard encryption.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	● Codecov Infrastructure Security ● Codecov Code Security ● Codecov Security Awareness
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	● Codecov Code Security ● Codecov Vulnerability Testing / Pentesting Sentry has a documented Disaster Recovery Plan that defines procedures to recover all resources and processes necessary for service and data recovery, including all information security aspects of business continuity management. Sentry has a documented Incident Response Plan, which establishes procedures to be undertaken in response to information security incidents.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	● Codecov Vulnerability Testing / Pentesting
Measures for user identification and authorization	● Codecov Code Security
Measures for the protection of data during transmission	Data transfers are secured using Transport Layer Security (TLS) and industry-standard encryption.
Measures for the protection of data during storage	● Codecov Infrastructure Security ● Codecov Code Security
Measures for ensuring physical security of locations at which personal data are processed	Sentry uses GCP to provide cloud hosting services for its production environment. The facilities, including the hardware and equipment therein, are maintained by GCP. The physical security, environmental controls and incident management for the facilities are also the

Technical and Organizational Measures	**Relevant Section(s) of Codecov Service Security Policy (if applicable)**
	responsibility of GCP. Additional information on GCP security measures are available here: https://cloud.google.com/docs/security/overview/whitepaper.
Measures for ensuring events logging	Sentry logs authentication, availability and error events and uses tools for infrastructure management.
Measures for ensuring system configuration, including default configuration	● Codecov Infrastructure Security ● Codecov Code Security
Measures for internal IT and IT security governance and management	● Codecov Security Compliance ● Sentry has dedicated teams responsible for architecting, building and owning security.
Measures for certification/assurance of processes and products	● Codecov Security Compliance
Measures for ensuring data minimization	Sentry retains raw/preprocessed coverage reports for 30 days. Options are provided for customers to request data removal.
Measures for ensuring data quality	● Codecov Infrastructure Security
Measures for ensuring limited data retention	Sentry retains raw/preprocessed coverage reports for 30 days. Options for customers to request data removal are provided.
Measures for ensuring accountability	● Codecov Security Awareness ● Codecov Responsible Disclosure Policy
Measures for allowing data portability and ensuring erasure	Customers can contact Sentry for a copy of their data and/or request data erasure.
Measures and assurances regarding U.S. government surveillance (“Additional Safeguards”)	● Sentry uses encryption both in transit and at rest. ● As of the date of this DPA, Sentry has not received any national security orders of the type described in Paragraphs 150-202 of the judgment in the EU Court of Justice Case C-311/18, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems. ● No court has found Sentry to be the type of entity eligible to receive process issued under FISA Section 702: (i) an “electronic communication service provider” within the meaning of 50 U.S.C § 1881(b)(4) or (ii) a member of any of the categories of entities described within that definition. ● Sentry shall not comply with any request under FISA for bulk surveillance, i.e., a surveillance demand whereby a targeted account identifier is not identified via a specific “targeted selector” (an identifier that is unique to the targeted endpoint of communications subject to the surveillance). ● Sentry shall use all available legal mechanisms to challenge any demands for data access through national security process that Sentry receives, as well as any non-disclosure provisions attached thereto. ● Sentry shall take no action pursuant to U.S. Executive Order 12333.

Technical and Organizational Measures	Relevant Section(s) of Codecov Service Security Policy (if applicable)
	● Sentry will notify Customer if Sentry can no longer comply with the Standard Contractual Clauses or these Additional Safeguards, without being required to identify the specific provision with which it can no longer comply.

Schedule 3

Cross-Border Transfer Mechanisms

1. Data Privacy Framework. Sentry complies with the Data Privacy Framework in relation to transfers of Personal Data from Europe to the United States. The parties agree that Sentry will use the Data Privacy Framework to lawfully receive European Personal Data in the United States and Sentry will ensure that we provide at least the same level of protection to such data as is required by the Data Privacy Framework Principles. Sentry will notify Customer if we make a determination that we can no longer comply with our obligations under the Data Privacy Framework.

2. Standard Contractual Clauses. In the event that the Data Privacy Framework is invalidated, or the Data Privacy Framework does not otherwise apply to the transfer of European Personal Data from Customer to Sentry, then the parties agree to be subject to, abide by, and process such European Personal Data in compliance with the SCCs as follows:

2.1 EEA Transfers. If the GDPR applies to the European Personal Data:

(i) Module 2 (Controller to Processor) applies where Customer is a Controller of European Personal Data and Sentry is a Processor of European Personal Data;

(ii) Module 3 (Processor to Processor) applies where Customer is a Processor of European Personal Data (on behalf of a third-party Controller) and Sentry is a Processor of European Personal Data;

(iii) Customer is the “data exporter” and Sentry is the “data importer”;

(iv) by entering into this DPA, each party is deemed to have signed the SCCs (including their Annexes) as of the effective date of this DPA; and

(v) for each Module, where applicable, the following applies:

(a) the optional docking clause in Clause 7 applies;

(b) in Clause 9, option 2 will apply, the minimum time period for prior notice of Subprocessor changes shall be as set out in Section 7.2 (List of Subprocessors) of this DPA and Sentry shall fulfill its notification obligations by notifying Customer of any Subprocessor changes in accordance with Section 7.2 (List of Subprocessors) of this DPA;

(c) in Clause 11, the optional language does not apply;

(d) in Clause 13, all square brackets are removed with the text remaining;

(e) in Clause 17, Option 1 will apply, and the SCCs will be governed by the laws of the Republic of Ireland;

(f) in Clause 18(b), disputes will be resolved before the courts of the Republic of Ireland; and

(g) Schedules 1 and 2 and Section 7.2 (List of Subprocessors) of this DPA contain the information required in Annex 1 and 2 of the SCCs.

2.2 UK Transfers. If the UK GDPR applies to the European Personal Data, the SCCs as incorporated under Section 2.1 (EEA Transfers) of this Schedule 3 shall apply with the following modifications: (i) the SCCs shall be amended as specified by the UK Addendum, which shall be incorporated by reference; (ii) Tables 1 to 3 in Part 1 of the UK Addendum shall be populated with the information from Schedules 1 and 2 and Section 7.2 (List of Subprocessors) of this DPA; (iii) Table 4 in Part 1 of the UK Addendum shall be deemed completed by selecting "importer"; and (iv) any conflict between the SCCs and the UK Addendum shall be resolved in accordance with Section 10 and Section 11 of the UK Addendum.

2.3 **Swiss Transfers**. If the Swiss FADP applies to the European Personal Data, the SCCs as incorporated under Section 2.1 (EEA Transfers) of this Schedule 3 shall apply with the following modifications: (i) references to "Regulation (EU) 2016/679" shall be interpreted as references to the Swiss FADP; (ii) references to "EU," "Union," and "Member State" shall be replaced with "Switzerland"; (iii) references to the "competent supervisory authority" and "competent courts" shall be interpreted as references to the "Swiss Federal Data Protection and Information Commissioner" and the "competent Swiss courts"; and (iv) the SCCs shall be governed by the laws of Switzerland and disputes shall be resolved before the competent Swiss courts.

2.4 **Additional Provisions**. Where this Section 2 applies, it is not the intention of either party to contradict or restrict any of the provisions set forth in the SCCs and, accordingly, if and to the extent the SCCs conflict with any provision of the Agreement (including this DPA), the SCCs shall prevail to the extent of such conflict. In particular, nothing in this DPA shall exclude the rights of third-party beneficiaries granted under the SCCs. You agree that in the event we cannot ensure compliance with the SCCs, we will inform you promptly and you will provide us with a reasonable period of time to cure any non-compliance. You will reasonably cooperate with us to agree what additional safeguards or measures, if any, may be reasonably required to cure the non-compliance and will only be entitled to suspend the transfer of European Personal Data and/or terminate the affected parts of the Service if we have not or cannot cure the non-compliance before the end of the cure period.

3. **Alternative Transfer Solution**. With respect to European Personal Data, you agree that if we adopt an alternative data transfer mechanism (including any new version of, or successor to, the SCCs or Data Privacy Framework adopted pursuant to applicable European Data Protection Legislation) for European Personal Data not described in this DPA ("**Alternative Transfer Solution**"), the Alternative Transfer Solution shall apply instead of the transfer mechanisms described in this DPA (but only to the extent such Alternative Transfer Solution complies with applicable European Data Protection Legislation and extends to the territories to which European Personal Data is transferred), and if we request that you take any action (including, without limitation, execution of documents) reasonably required to give full effect to that solution, you will promptly do so.

Schedule 4

Jurisdiction Specific Terms

1. Europe

1.1 Additional Information. You acknowledge that Sentry is required under European Data Protection Legislation (i) to collect and maintain records of certain information, including, among other things, the name and contact detail of each Processor and/or Controller on whose behalf we are acting and, where applicable, of such Processor's or Controller's local representative and data protection officer; and (ii) to make such information available to the supervisory authorities. Accordingly, if European Data Protection Legislation applies to the processing of Personal Data, you will, when requested, provide this additional information to us, and ensure that the information is kept accurate and up-to-date.

2. California.

2.1 Definitions. For purposes of Section 2 (California) of this Schedule 4:

2.1.1 "business purpose", "commercial purpose", "personal information", "sell", "service provider" and "share" have the meanings given in the CCPA.

2.1.2 The definition of "Data Subject" includes "consumer" as defined under the CCPA.

2.1.3 The definition of "Controller" includes "business" as defined under the CCPA.

2.1.4 The definition of "Processor" includes "service provider" as defined under the CCPA.

2.2 Obligations.

2.2.1 Customer is providing the Personal Data to Sentry under the Agreement for the limited and specific business purposes of providing the Service as described in Schedule 1 to this DPA and otherwise performing under the Agreement.

2.2.2 Sentry will comply with its applicable obligations under the CCPA and provide the same level of privacy protection to Personal Data as is required by the CCPA.

2.2.3 Sentry acknowledges that Customer has the right to: (i) take reasonable and appropriate steps under Section 4.4 (Audit Rights) of this DPA to help to ensure that Sentry's use of Personal Data is consistent with Customer's obligations under the CCPA, (ii) receive from Sentry notice and assistance under Section 5.2 (Cooperation; Data Subjects' Rights) of this DPA regarding consumers' requests to exercise rights under the CCPA and (iii) upon notice, take reasonable and appropriate steps to stop and remediate unauthorized use of Personal Data.

2.2.4 Sentry will notify Customer promptly after it makes a determination that it can no longer meet its obligations under the CCPA.

2.2.5 Sentry will not retain, use or disclose Personal Data: (i) for any purpose, including a commercial purpose, other than the business purposes described in Section 2.2.1 of this Section 2 (California) of Schedule 4 or (ii) outside of the direct business relationship between Sentry with Customer, except, in either case, where and to the extent permitted by the CCPA.

2.2.6 Sentry will not sell or share Personal Data received under the Agreement.

2.2.7 Sentry will not combine Personal Data with other personal information except to the extent a service provider is permitted to do so by the CCPA.