SENTRY

MENU

BACK TO ALL LEGAL DOCS

Business Associate Amendment

Data Processing Addendum

- Data Encryption
- Data Retention
- Data Removal
- PII Scrubbing
- Application Security
- Multi-Factor Authentication
- Single Sign-On
- SAML 2.0
- REST API Authentication (API Key)
- Email Security
- Audit Controls
- Secure Application Development (Application Development Lifecycle)
- Corporate Security
- Malware Protection
- Risk Management
- Contingency Planning
- Security Policies
- Background Checks
- Security Training
- Disclosure Policy

Data Processing Addendum

Version

5.0.0

of This Agreement was created on December 29, 2022 .

Read what has changed

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 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 Data Protection Act of 19 June 1992 and its Ordinance ("Swiss DPA"); 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 to Sentry outside of Europe, and European Data Protection Legislation applies to the transfer (collectively, "Transferred Personal Data"), 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 set forth on Schedule 5. We may update this list 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 Schedule 5. 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.

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 provided by Customer in the Service

Contact person's name, position and contact details: Customer's contact details as provided by Customer in the Service

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

Technical and Organizational Measures	Relevant Section(s) of Sentry Service Security Policy (see below)
Measures of pseudonymization and encryption of personal data	• Data Flow – Data into System • Data Flow – Data through System • Data Security and Privacy – Data Encryption

Technical and Organizational Measures	Relevant Section(s) of Sentry Service Security Policy (see below)
	• 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

Technical and Organizational Measures	Relevant Section(s) of Sentry Service Security Policy (see below)
	• 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 Lifecycle)

Technical and Organizational Measures	Relevant Section(s) of Sentry Service Security Policy (see below)
	• 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

Technical and Organizational Measures	Relevant Section(s) of Sentry Service Security Policy (see below)
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

Technical and Organizational Measures	Relevant Section(s) of Sentry Service Security Policy (see below)
	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. • Sentry publishes a transparency report indicating the types of binding legal demands for the personal data it has received, including national security orders and

Technical and Organizational Measures	Relevant Section(s) of Sentry Service Security Policy (see below)
	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.

Sentry Service Security Policy

(Current version is at https://sentry.io/security/, version as of December 7, 2022 is below)

Security & Compliance

Security and compliance are top priorities for Sentry because they are fundamental to your experience with the product. Sentry is committed to securing your application's data, eliminating systems vulnerability, and ensuring continuity of access.

Sentry uses a variety of industry-standard technologies and services to secure your data from unauthorized access, disclosure, use, and loss. All Sentry employees undergo background checks before employment and are trained on security practices during company onboarding and on an annual basis.

Security is directed by Sentry's Chief Technology Officer and maintained by Sentry's Security & Operations team.

Infrastructure and Network Security

Physical Access Control

Sentry is hosted on Google Cloud Platform. Google data centers feature a layered security model, including extensive safeguards such as:

- Custom-designed electronic access cards
- Alarms
- Vehicle access barriers
- Perimeter fencing
- Metal detectors
- Biometrics

According to the Google Security Whitepaper: Google data centers also implement "security measures such as laser beam intrusion detection and 24/7 monitoring by high-resolution interior and exterior cameras" to detect and track intruders. In addition, "access logs, activity records, and camera footage are available in case an incident occurs" and "experienced security guards, who have undergone rigorous background checks and training, routinely patrol" Google data centers.

Sentry employees do not have physical access to Google data centers, servers, network equipment, or storage.

Logical Access Control

Sentry is the assigned administrator of its infrastructure on Google Cloud Platform, and only designated authorized Sentry operations team members have access to configure the infrastructure on an as-needed basis behind a two-factor authenticated virtual private network. Specific private keys are required for individual servers, and keys are stored in a secure and encrypted location.

Penetration Testing

Sentry undergoes annual penetration testing conducted by an independent, third-party agency. For testing, Sentry provides the agency with an isolated clone of sentry.io and a high-level diagram of application architecture. No customer data is exposed to the agency through penetration testing.

Information about any security vulnerabilities successfully exploited through penetration testing is used to set mitigation and remediation priorities. A summary of penetration test findings is available to customers via their Sentry account or upon request.

Third-Party Audit

Google Cloud Platform undergoes various third-party independent audits regularly and can provide verification of compliance controls for its data centers, infrastructure, and operations. This includes, but is not limited to, the SSAE 18-compliant SOC 2 certification and ISO 27001 certification. Sentry undergoes regular third-party independent audits on a regular basis and Sentry's SOC 2 report and ISO 27001 certificate are available to customers via their Sentry account or upon request.

Intrusion Detection and Prevention

Unusual network patterns or suspicious behavior are among Sentry's most significant concerns for infrastructure hosting and management. Sentry and Google Cloud Platform's intrusion detection and prevention systems (IDS/IPS) rely on both signature-based security and algorithm-based security to identify traffic patterns that are similar to known attack methods.

IDS/IPS involves tightly controlling the size and make-up of the attack surface, employing intelligent detection controls at data entry points, and developing and deploying technologies that automatically remedy dangerous situations, as well as preventing known threats from accessing the system in the first place.

Sentry does not provide direct access to security event forensics but does provide access to the engineering and customer support teams during and after any unscheduled downtime.

Business Continuity and Disaster Recovery

High Availability

Every part of the Sentry service uses properly-provisioned, redundant servers (e.g., multiple load balancers, web servers, replica databases) in the case of failure. As part of regular maintenance, servers are taken out of operation without impacting availability.

Business Continuity

Sentry keeps hourly encrypted backups of data in multiple regions on Google Cloud Platform. While never expected, in the case of production data loss (i.e., primary data stores lost), we will restore organizational data from these backups.

Disaster Recovery

In the event of a region-wide outage, Sentry will bring up a duplicate environment in a different Google Cloud Platform region. The Sentry operations team has extensive experience performing full region migrations.

Data Flow

Data into System

SDKs securely send events, containing information on errors and exceptions, to the Sentry server, which processes and stores the events. Audit data of processing and storing is transmitted to our in-house logging infrastructure through encrypted connections.

We believe SDKs should provide some mechanism for proactively scrubbing data, ideally through an extensible interface that the user can customize. Sentry

provides documentation outlining SDK configuration to filter out bits of data for security and privacy purposes, but that otherwise delivers the rest of the event data intact. Scrubbing the following values is recommended:

- Values where the keyname matches password, passwd, or secret
- Values that match the regular expression of r'^(?:\d[-]*?){13,16}\$' (credit card-like)
- Session cookies
- Authentication header (HTTP)

Data through System

Data is sent securely to Sentry via TLS to an HTTPS endpoint. All data is AES-256bit encrypted, both in transit and at rest. Sentry aggregates events along with contextual data related to the user's environment, preceding events, and the release and deployment changeset. Events data is also enriched with artifacts like source maps or symbols uploaded by the user or sourced externally.

Sentry's latest SSL Labs Report can be found here.

Data out of System

Once the event is processed, it can then be accessed via Sentry's user interface and REST APIs. Sentry integrates with a variety of third-party tools so developers can combine error data from Sentry with data from other systems, manage workflows efficiently, and be alerted of errors through notification and chat tools, in addition to email and SMS. Therefore, Sentry's high standards for security and compliance also extend to its partner network.

Data Security and Privacy

Data Encryption

All data in Sentry servers is encrypted at rest. Google Cloud Platform stores and manages data cryptography keys in its redundant and globally distributed Key

Management Service. So, if an intruder were ever able to access any of the physical storage devices, the Sentry data contained therein would still be impossible to decrypt without the keys, rendering the information a useless jumble of random characters.

Encryption at rest also enables continuity measures like backup and infrastructure management without compromising data security and privacy.

Sentry exclusively sends data over HTTPS transport layer security (TLS) encrypted connections for additional security as data transits to and from the application.

Data Retention

Sentry retains event data for 90 days by default, regardless of plan. We remove individual events after 90 days, and we remove aggregate issues after 90 days of inactivity. All event data and most metadata are eradicated from the service and from the server without additional archiving in order to prevent the threat of intrusion.

Data Removal

All customer data stored on Sentry servers is eradicated upon a customer's termination of service and deletion of account after a 24-hour waiting period to prevent accidental cancellation. Data can also be deleted upon request and via Sentry's REST API and UI.

Users have the ability to remove events via bulk deletion of all events within an issue and can permanently remove data related to a given tag.

PII Scrubbing

We recommend that users do not send any personally identifiable information (PII) to Sentry. To mitigate accidents and other security risks, Sentry offers server-side filtering as a default setting. The Data Scrubber option in Sentry's settings

automatically removes values that appear to be sensitive information so that it will not be stored on Sentry's servers.

Additionally, users can specify values to be scrubbed in the Project Settings. IP Address storage can also be disabled. The latter is particularly important if you're concerned about PII and using Sentry's Browser JavaScript SDK.

Application Security

Multi-Factor Authentication

In addition to password login, multi-factor authentication (MFA) provides an added layer of security to Sentry. We encourage MFA as an important step towards securing data access from intruders. Sentry users can deploy universal second-factor devices like YubiKeys (which can also be used to confirm the sudo prompt) or time-based one-time password (TOTP) apps like Google Authenticator as additional factors. This also applies to sign-in with an SSO provider.

Sentry's organization list also displays who has MFA enabled so users can vet their own organization's security.

Single Sign-On

Sentry's single sign-on (SSO) implementation prioritizes security. We aggressively monitor linked accounts and disable them with any reasonable sign that the account's access has been revoked. SSO also improves user experience by streamlining login and improving access from trusted domains. Sentry currently offers SSO via Google Business Apps and GitHub Organizations.

SAML 2.0

To facilitate user authentication through the web browser and improve identity management, Sentry offers Security Assertion Markup Language (SAML)-based SSO and System Cross-Domain Identity Management (SCIM) as standard features to customers on its Business and Enterprise plans. SAML 2.0 enhances user-

based security and streamlines signup and login from trusted portals to enhance user experience, access management, and auditability. SCIM enables automated account provisioning.

Sentry integrates with SAML 2.0 and SCIM providers including Azure Active Directory and Okta.

REST API Authentication (API Key)

Sentry's REST API uses an auth token for authentication. Authentication tokens are passed using the auth header and are used to authenticate a user account with the API.

We strongly recommend using organization-wide authentication tokens.

Email Security

The Sentry service includes email notifications and reports. Sender policy framework (SPF) is a system to prevent email address spoofing and minimize inbound spam. We have SPF records set through Dyn, our domain name service (DNS), and domain-based message authentication, reporting, and conformance (DMARC) set up for monitoring reports to prevent the possibility of phishing scams. Sentry users can see the TXT records on dmarc.sentry.io and sentry.io:

```
\$ dig \_dmarc.sentry.io TXT +short

"v=DMARC1; p=reject; fo=1; aspf=r; pct=100; rua=mailto:dmarc_agg@vali

\$ dig sentry.io TXT +short | grep spf

"v=spf1 include:_spf.google.com include:mail.zendesk.com include:send
```

Audit Controls

We know user administration is central to security and management, and auditing user logs is often the first step in both an emergency response plan and policy compliance requirements. All Sentry customers get admin controls governing identity, access, and usage to keep your data safe, secure, and centrally managed.

Membership within Sentry is handled at the organization level. The system is designed so each user has a singular account that can be reused across multiple organizations (even those using SSO). Each Sentry user should have their own account and can choose their own personal preferences and notifications settings. Access to organizations is dictated by role:

- Billing
- Member
- Admin
- Manager
- Organization Owner

For any organization on a Sentry plan, the project administration portal is the hub for seeing and managing users and usage. The member list includes the username, email, status, added date, teams, and role for each user. The admin or owner can revoke access by project, team, or org and change the user role. Additionally, the admin can request login and password history and revoke passwords and active sessions for any user via request to Sentry Support.

In the audit log, all of the actions by user and event within the Sentry UI (e.g., member.invite, project.create) are listed chronologically by time and IP address so you'll always have a view into your organization's most recent history.

Secure Application Development (Application Development Lifecycle)

Sentry practices continuous delivery, which means all code changes are committed, tested, shipped, and iterated on in a rapid sequence. A continuous delivery methodology, complemented by pull request, continuous integration (CI),

and automated error tracking, significantly decreases the likelihood of a security issue and improves the response time to and the effective eradication of bugs and vulnerabilities. Release notes and details for Sentry and its SDKs can be found on their respective GitHub release pages (e.g., Sentry releases and raven-js releases).

Corporate Security

Malware Protection

At Sentry, we believe that good security practices start with our own team, so we go out of our way to protect against internal threats and local vulnerabilities. All company-provided workstations are enrolled in Mobile Device Management (MDM) and Endpoint Detection and Response (EDR) solutions to enforce security settings including full-disk encryption, screen lock, and OS updates.

Risk Management

Sentry follows the risk management procedures outlined in NIST SP 800-30, which include nine steps for risk assessment and seven steps for risk mitigation.

All Sentry product changes must go through code review, CI, and build pipeline to reach production servers. Only designated employees on Sentry's operations team have secure shell (SSH) access to production servers.

We perform testing and risk management on all systems and applications on a regular and ongoing basis. New methods are developed, reviewed, and deployed to production via pull request and internal review. New risk management practices are documented and shared via staff presentations on lessons learned and best practices.

Sentry performs risk assessments throughout the product lifecycle per the standards outlined in HIPAA Security Rule, 45 CFR 164.308:

- Before the integration of new system technologies and before changes are made to Sentry physical safeguards

- While making changes to Sentry physical equipment and facilities that introduce new, untested configurations
- Periodically as part of technical and non-technical assessments of the security rule requirements as well as in response to environmental or operational changes affecting security

Contingency Planning

The Sentry operations team includes service continuity and threat remediation among its top priorities. We keep a contingency plan in case of unforeseen events, including risk management, disaster recovery, and customer communication sub-plans that are tested and updated on an ongoing basis and thoroughly reviewed for gaps and changes at least annually.

Security Policies

Sentry maintains an internal wiki of security policies, which is updated on an ongoing basis and reviewed annually for gaps. An overview of specific security policies is available to Sentry enterprise customers upon request:

- Access Management
- Change Management
- Data Request
- Data Management
- Information Security
- Incident Response
- Policy Management and Maintenance
- Risk Management
- Vendor Management
- Vulnerability Management

Background Checks

Sentry conducts background checks for all new hires, including verification on the following:

- Identity verification
- Global watchlist check
- National criminal records check
- County criminal records check
- (U.S. only) Sex offender registry check

Security Training

All new employees receive onboarding and systems training, including environment and permissions setup, formal software development training (if pertinent), security policies review, company policies review, and corporate values and ethics training.

All employees additionally complete security training at least once a year. Policies presented to employees as part of the onboarding process are reviewed once a year to ensure we are keeping up with best practices.

Disclosure Policy

Sentry follows the incident handling and response process recommended by SANS, which includes identifying, containing, eradicating, recovering from, communicating, and documenting security events. Sentry notifies customers of any data breaches as soon as possible via email and phone call, followed by multiple periodic updates throughout each day addressing progress and impact. Sentry Enterprise plans include a dedicated customer success manager who holds responsibility for customer communication, as well as regular check-ins and escalations.

Sentry maintains a live report of operational uptime and issues on our status page. Anyone can subscribe to updates via email from the status page. Any known incidents are reported there, as well as on our Twitter feed.

Vulnerability Disclosure

Anyone can report a vulnerability or security concern with a Sentry product by contacting security@sentry.io and including a proof of concept, a list of tools used (including versions), and the output of the tools. We take all disclosures very seriously, and once we receive a disclosure we rapidly verify each vulnerability before taking the necessary steps to fix it. Once verified, we periodically send status updates as problems are fixed.

To encrypt sensitive information that is sent to us, our PGP key can be found on keyservers with the fingerprint:

```
E406 C27A E971 6515 A1B1 ED86 641D 2F6C 230D BE3B
```

Other Resources

Compliance Certifications

Sentry has obtained the following compliance certifications:

- SOC2 Type I
- SOC2 Type II
- HIPAA Attestation
- ISO 27001

If you already use Sentry, you can access the report and certificate via your Sentry account. Otherwise, contact us for a copy of any report(s) you're interested in reading (it'll be less infuriating than your social feed.)

Codecov Service

Technical and Organizational Measures	Relevant Section(s) of Codecov Service Security Policy (if applicable) (see below)
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	Codecov Code Security

Technical and Organizational Measures	Relevant Section(s) of Codecov Service Security Policy (if applicable) (see below)
authorization	
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 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.

Technical and Organizational Measures	Relevant Section(s) of Codecov Service Security Policy (if applicable) (see below)
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) (see below)
	• 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 Policy

(Current version is at https://about.codecov.io/security/, version as of October 11, 2022 is below)

Codecov Infrastructure Security

- Codecov utilizes GCP (Google Cloud Platform) for our cloud-based products, Terraform for IaC (Infrastructure as Code), and Docker/Kubernetes for microservices. See Google's SOC3 report here.
- Docker images are squashed and/or multistaged to prevent docker layer attacks.
- All publicly available assets hosted in GCP, virtual servers in GCP, and employee endpoints are vulnerability scanned on a daily basis. Tickets for vulnerabilities are automatically created and assigned a due date based on our IR (Incident Response) policy SLA (< 30 days for Critical and High, < 60 days for Medium, < 120 days for Low).
- All GCP Kubernetes nodes and employee endpoints run EDR (Endpoint Detection and Response) agents configured to quarantine any malware detected and log to our cloud-based SIEM.
- Use of SSO and endpoint compliance monitoring tools to ensure 2FA is used whenever possible and endpoints are full disk encrypted, screen-lock enabled, etc.

Codecov Code Security

- Codecov utilizes numerous tools to detect vulnerabilities and protect our code, including:
    - Static application security testing (SAST)
    - Dynamic application security testing (DAST)
    - Repository dependency scanning
    - Scanning repos for secrets (API keys, passwords, etc) to ensure they are not stored or hard coded in our code base.
    - Usage of GCP's Secret Manager and environment variables for proper secret protection and inclusion at runtime.
    - All commits to Codecov repos are GPG signed and require a code review before merging.
    - All Codecov code repositories are only accessible via employee specific accounts registered to the @codecov.io domain.
    - All commits to repos that have security relevant changes undergo a code review by our Security Team.
    - 2FA is enabled for access to our code base, with 2FA and VPN required for access to our GCP resources.
    - All Codecov uploader binaries are SHA256 signed, and changes to uploader binaries are monitored and immediately reported to staff. For instructions on how to verify uploader binaries, see here.

Codecov Vulnerability Testing/Pentesting

- Codecov undergoes third party vulnerability/pentesting to support our SOC2 compliance efforts.
- Codecov also performs internal network and application security scanning as follows:
    - Daily network and host-based vulnerability scanning for endpoints, virtual servers in GCP, and publicly accessible assets in GCP

Codecov Security Awareness

- Codecov requires yearly security awareness training for all staff.
- Secure coding training for development, security, and devops teams is given yearly.

Codecov Responsible Disclosure Policy

Data security is a top priority for Codecov, and Codecov believes that working with skilled security researchers can identify weaknesses in any technology.

Even though we don't have a bug bounty program, we will ensure that your findings get passed along to the security team for remediation if you've found a security vulnerability in Codecov's service.

Disclosure Policy

- If you believe you've discovered a potential vulnerability, please let us know by emailing us at security@codecov.io. We will acknowledge your email within five business days.
- Provide us with a reasonable amount of time to resolve the issue before disclosing it to the public or a third party. We aim to resolve critical issues within five business days of disclosure.
- Make a good faith effort to avoid violating privacy, destroying data, or interrupting or degrading the Codecov service. Please only interact with accounts you own or for which you have explicit permission from the account holder.

Exclusions

While researching, we'd like you to refrain from:

- Distributed Denial of Service (DDoS)
- Spamming
- Social engineering or phishing of Codecov employees or contractors
- Any attacks against Codecov's physical property or data centers

Thank you for helping to keep Codecov and our users safe!

Changes

We may revise these guidelines from time to time. The most current version of the guidelines will be available at https://codecov.io/security

Contact

Codecov is always open to feedback, questions, and suggestions. If you would like to talk to us, please feel free to email us at security@codecov.io, and our PGP key is at https://codecov.io/.well-known/security.txt.

Responsibility

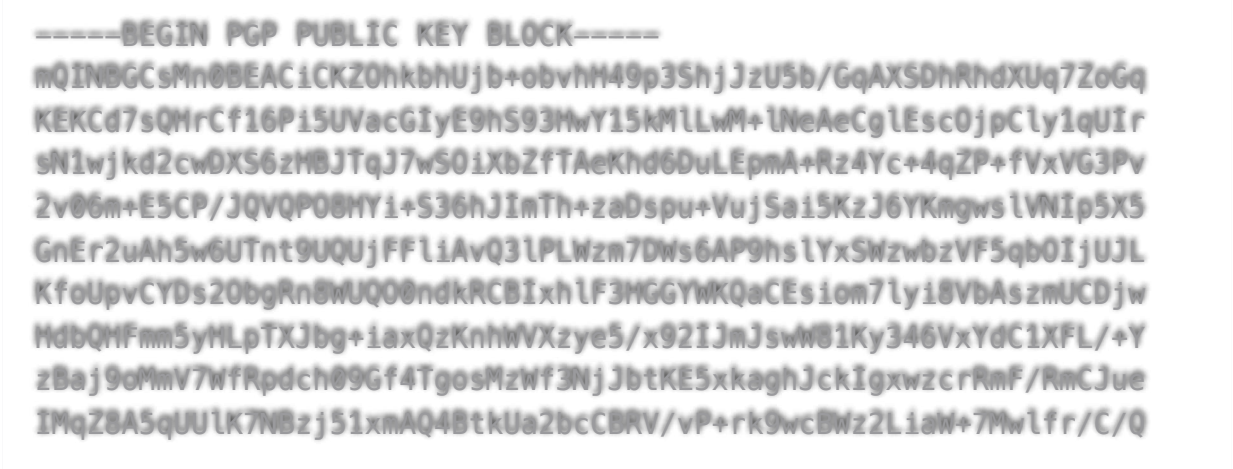
It is the Security Team's responsibility to see this policy is enforced. Last updated: October 11, 2022

For questions and feedback, contact security@codecov.io

Current PGP Public Keys

Codecov's current PGP public key can be fetched from Keybase or from most keyservers with the key ID ED779869 and fingerprint 2703 4E7F DB85 0E0B BC2C 62FF 806B B28A ED77 9869 it can also be found below:

Current Key



Swvv/JW2LsQ4iWc1BY7m7ksn9dcdypEq/1JbIzVLCRDG7pbMj9yLgYmhe5TtjOM3
ygk25584EhXSgUA3MZw+DIqhbMQBYgrKndTr2N/wuBQY62zZg1YGQByD4QARAQAB
tEpDb2RlY292IFVwbG9hZGVyIChDb2RlY292IFVwbG9hZGVyIFZlcmlmaWNhdGlv
biBLZXkpIDxzZWN1cml0eUBjb2RlY292LmlvPokCTgQTAQoAOBYhBCcDTn/bhQ4L
vCxi/4Brsortd5hpBQJgrDJ9AhsDBQsJCAcCBhUKCQgLAgQWAgMBAh4BAheAAAoJ
EIBrsortd5hpxLMP/3Fbgx5EG7zUUOqPZ+Ya9z8JlZFIkh3FxYMfMFE8jM9Es26F
V2ZTJL0259MxM+5N0XzObi3h4XqIzBn42pDRfwtojY5wl2STJ9Bzu+ykPog7OB1u
yfWXDRKcqPTUIxI1/WdU+c0/WNE6wjyzK+lRc1YUlp4pdNU7l+j2vKN+jGi2b6nV
PTPRsMcwy3B90fKf5h2wNMNqO+KX/rjgpG9Uhej+xyFWkGM1tZDQQYFj+ugQUj61
BMsQrUmxOnaVVnix21cHnACDCaxqgQZM3iZyEOKPNMsRFRP+0fLEnUMP+DVnQE6J
Brk1Z+XhtjGI9PISQVx5KKDKscreS/D5ae2Cw/FUlQMf57kir6mkbZVhz2khtccz
atD0r59WomNywIDyk1QfAKV0+O0WeJg8A69/Jk6yegsrUb5qEfkih/I38vvI0OVL
BYve/mQIMuQo5ziBptNytCrN5TXMXzguX9GOW1V1+3DR+w/vXcnz67sjlYDysf1f
JUZv9edZ2RGKW7agbrgOw2hB+zuWZ10tjoEcsaSGOLtKRGFDfmu/dBxzl8yopUpa
Tn79QKOieleRm5+uCcKCPTeKV0GbhDntCZJ+Yiw6ZPmrpcjDowAoMQ9kiMVa10+Q
WwwoaRWuqhf+dL6Q2OLFOxlyCDKVSyW0YF4Vrf3fKGyxKJmszAL+NS1mVcdxuQIN
BGCsMn0BEADLrIesbpfdAfWRvUFDN+PoRfa0ROwa/JOMhEgVsowQuk9No8yRva/X
VyiA6oCq6na7IvZXMxT7di4FWDjDtw5xMjbtFg336IJTGBcnzm7WIsjvyyw8kKfB
8cvG7D2OkzAUF8SVXLarJ1zdBP/Dr1Nz6F/gJsx5+BM8wGHEz4DsdMRV7ZMTVh6b
PaGuPZysPjSEw62R8MFJ1fSyDGCKJYwMQ/sKFzseNaY/kZVR5lq0dmhiYjNVQeG9
MJ6ZCGSGT5PKNOwx/UEkT6jhvzWgfr2eFVGJTcdwSLEgIrJIDzP7myMGxuOiuCmJ
ENgL1f7mzGkJ/hYXq1RWqsn1Fh2I9KZMMggqu4a+s3RiscmNcbIlIhJLXoE1bxZ/
TfYZ9Aod6Bd5TsSMTZNwV2am9zelhDiFF60FWww/5nEbhm/X4suC9W86qWBxs3Kh
vk1dxhElRjtgwUEMA5OfOO48ERMfR7COM719D/YmqLU3EybBgJbGoC/yjlGJxv0R
kOMAiG2FneNKEZZihReh8A5Jt6jYrSoMFRwL6oJIZfLezB7Rdajx1uM7uYcUyIaE
SiDWlkDw/IFM315NYFA8c1TCSIfnabUYaAxSLNFRmXnt+GQpm44qAK1x8EGhY633
e5B4FWorIXx0tTmsVM4rkQ6IgAodeywKG+c2Ikd+5dQLFmb7dW/6CwARAQABiQI2
BBgBCgAgFiEEJwNOf9uFDgu8LGL/gGuyiu13mGkFAmCsMn0CGwwACgkQgGuyiu13
mGkYWxAAkzF64SVpYvY9nY/QSYikL8UMlyyqirs6eFZ3Mj9lMRpHM2Spn9a3c701
0Ge4wDbRP2oftCyPP+p9pdUA77ifMTlRcoMYX8oXAuyE5RT2emBDiWvSR6hQQ8bZ
WFNXal+bUPpaRiruCCUPD2b8Od1ftzLqbYOosxr/m5Du0uahgOuGw6zlGBJCVOo7
UB2Y++oZ8P7oDGF722opepWQ+bl2a6TRMLNWWlj4UANknyjlhyZZ7PKhWLjoC6MU
dAKcwQUdp+XYLc/3b00bvgju0e99QgHZMX2fN3d3ktdN5Q2fqiAi5R6BmCC04ISF
o5j10gGU/sdqGMvNhv5C21ibun7MEzMtxBhnhGmytfBJzrsj7GOReePsfTLoCoUq
dFMOAVUDciVfRtL2m8cv42ZJOXtPfDjsFOf0AKJk40/tc8mMMqZP7RVBr9RWOoq5
y9D37NfI6UB8rPZ6qs0a1Vfm8lIh2/k1AFECduXgftMDTsmmXOgXXS37HukGW7AL
QKWiWJQF/XopkXwkyAYpyuyRMZ77oF7nuqLFnl5VVEiRo0Fwu45erebc6ccSwYZU
8pmeSx7s0aJtxCZPSZEKZ3mn0BXOR32Cgs48CjzFWf6PKucTwOy/YO0/4Gt/upNJ
3DyeINcYcKyD08DEIF9f5tLyoiD4xz+N23ltTBoMPyv4f3X/wCQ=
=ch7z
-----END PGP PUBLIC KEY BLOCK-----

Terms

- Codecov: Codecov and its technology/product/services
- Service: One of the following companies: GitHub, Bitbucket or GitLab
- Team: A team or organization in Service
- Repo: A Service (public or private) repository
- User: A single person who has logged into Codecov via Service therefore has an active user session
- Guest: A http request performed without an active user sessions
- Worker: Codecov's sync back-end which handles uploading, report processing, and other tasks
- Bot: The User who was chosen to consume Service endpoints during Worker tasks
- Web: Codecov front-end service that handles page builds and all HTTP requests (GET, POST, etc.)
- Extension: The Codecov Browser Extension
- Token: A Users Oauth2 auth token/secret granted by Service upon logging-in to Codecov
- Scope: What level of permission a User has on a Repository in Service, provided by Services
- CI: continuous integration provider. Including (not limited to) Travis-CI, Circle CI, Jenkins, etc.
- API: HTTP requests to Service
- 3rd Party: A SaaS tool used by Codecov. Examples – Rippling and Tenable IO

Schedule 3

Cross-Border Transfer Mechanisms

1. **European Economic Area Transfers.** If the GDPR applies to the Transferred Personal Data:

1.1 The Standard Contractual Clauses are hereby incorporated by reference as follows:

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

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

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

(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.

1.2 For each Module, where applicable, the following applies:

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

(ii) 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;

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

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

(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 will be resolved before the courts of the Republic of Ireland; and

(vii) 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.

1.3 It is not the intention of either party to contradict or restrict any of the provisions set forth in the Standard Contractual Clauses and, accordingly, if and to the extent the Standard Contractual Clauses conflict with any provision of the Agreement (including this DPA), the Standard Contractual Clauses 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 Standard Contractual Clauses. You agree that in the event we cannot ensure compliance with the Standard Contractual Clauses, 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 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.

1.4 For so long as Sentry is self-certified to the Privacy Shield we shall continue to process Transferred Personal Data in compliance with the Privacy Shield Principles. With respect to Transferred Personal Data, you agree that if we adopt an alternative data transfer mechanism (including any new version of, or successor to, the Standard Contractual Clauses or Privacy Shield adopted pursuant to applicable European Data Protection Legislation) for Transferred 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 Transferred 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.

2. **UK Transfers**. If the UK GDPR applies to the Transferred Personal Data, the SCCs as incorporated under Section 1 (European Economic Area 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.

3. **Swiss Transfers**. If the Swiss DPA applies to the Transferred Personal Data, the SCCs as incorporated under Section 1 (European Economic Area 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 DPA; (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.

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.

Schedule 5

Subprocessor List

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

Sentry Service:

The Subprocessor list for the Sentry Service is available at https://sentry.io/legal/subprocessors/ or such other website as Sentry may designate. Customer must subscribe to receive notice under Section 7.2 of this DPA via the mechanism on the website.

Codecov Service:

The Subprocessor list for the Codecov Service is set forth below.

Third Party

Name	Address	Processing Purpose
Google LLC (Google Cloud Platform)	1600 Amphitheatre Parkway Mountain View, CA 94043 United States	Cloud infrastructure services
Elasticsearch AS	Postboks 539 1373 Asker Norway NO 994 812 564 MVA	Security information and event management

Affiliates

Name	Address	Processing Purpose
Functional Software GmbH	Rothschildplatz 3 Top 3.02.AB 1020 Vienna Austria	Provides parts of the Service and related technical support
Sentry Software Canada Inc.	129 Spadina Ave, 7th Floor Toronto, ON M5V 2L3 Canada	Provides parts of the Service and related technical support
Sentry Software Netherlands B.V.	Schiphol Boulevard 359 WTC Schiphol Airport, D-Tower 11th floor 1118BJ Schiphol Netherlands	Provides parts of the Service and related technical support
Codecov LLC	45 Fremont Street, Floor 8 San Francisco, CA 94105	Provides parts of the Service and related technical support

SUPPORT

RESOURCES

ANSWERS

Platforms

JAVASCRIPT	.NET	PYTHON
ANDROID	PHP	DJANGO
JAVA	FLASK	RUBY
LARAVEL	IOS	RAILS
NODE	REACT	GO

SEE ALL >

TWITTER GITHUB DRIBBBLE LINKEDIN