How to Comply with GDPR

SENTRY

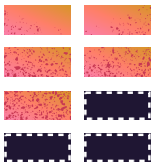
How to Comply with GDPR

If you include EU personal data in the service data you configure to be collected and reported to Sentry, you must comply with GDPR. This document highlights key GDPR requirements, how Sentry can help you with compliance, and additional steps you may need to take.

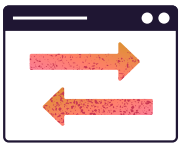
Summary of Key GDPR Compliance Steps

1 **Entering into GDPR-compliant contract terms**

2 **Controlling and minimizing personal data**



3 **Knowing your data transfers**



4 **Understanding Sentry's security configurations**

5 **Obtaining required notices and consents**

6 **Managing data subject requests**

1 ***Lawful Processing*** *— Have in place GDPR-compliant contractual terms with your processors — the third parties that handle EU personal data on your behalf.*

How does Sentry meet GDPR obligations?

Sentry makes available a Data Processing Addendum, with contractual terms that govern both your and Sentry's rights and responsibilities for the data, as required under GDPR. This includes our commitment to handle the data in accordance with your instructions as your processor.

WHAT DO YOU NEED TO DO?

- ☐ **Enter into data processing terms with Sentry**. You can agree to our Data Processing Addendum by following our Help Center instructions.*
- ☐ **Account for other processors**. Determine whether you need data processing terms in place with your other processors.

**Enterprise customers can reach out to their Sentry Sales contact to discuss additional options.*

2 ***Data Minimization*** *— Limit data processing to what is necessary for your purposes*

How does Sentry meet GDPR obligations?

Sentry has built-in tools and functionalities to enable you to control and manage the data you send to Sentry, including through Sentry's configurable SDKs and data scrubbers.

WHAT DO YOU NEED TO DO?

You control the data you send to Sentry, and are responsible for minimizing personal data to what is necessary for your purposes.

- ☐ **Configure Sentry SDKs**. Control the personal data you send to Sentry by configuring our SDKs. See also our product documentation.
- ☐ **Use our data scrubbing tools**. Use our various data scrubbing tools to remove personal data before it is ever sent to Sentry (or to prevent personal data from being stored by Sentry after it is sent).
- ☐ **Customize privacy settings**. Customize Sentry privacy settings for relevant products such as Session Replay. While our Session Replay product is set to mask, redact, and block certain data fields by default, you can update these settings based on your use case and needs.
- ☐ **Use Sentry Relay**. Sentry makes available Sentry Relay, a free**, standalone application that can act as a middle layer between you and Sentry. You configure Sentry SDKs to send your service data to Sentry Relay, and then scrub personal data from within your own infrastructure before sending to Sentry.
- ☐ **Review Sentry source code**. You can better understand how Sentry and Sentry SDKs work by looking into our source code.

**Sentry Relay in managed mode is only available for qualifying plans.

3 ***Data Transfer*** *- Have a valid mechanism for data transfers out of the EU*

How does Sentry meet GDPR obligations?

- EU-U.S. DPF. Sentry participates in and relies on the EU-U.S. Data Privacy Framework (EU-U.S. DPF) , which has been deemed a valid mechanism for EU-U.S. data transfers by the European Commission. You can find us listed as a participant on the Data Privacy Framework website.

- EU Standard Contractual Clauses. To the extent EU-U.S. DPF cannot apply to the transfer of your data to the U.S., including if invalidated by the EU courts, we offer the EU Standard Contractual Clauses as an alternative mechanism and provide information on International Data Transfers with Sentry to allow you to conduct your own due diligence.

- Other storage options. Sentry gives you an option to store your data in the EU instead of the U.S. Learn more about this option, and what it means for data storage and processing in our EU region documentation.

WHAT DO YOU NEED TO DO?

- ☐ **Conduct your own diligence**. Review the EU Standard Contractual Clauses incorporated into our Data Processing Addendum as an alternative transfer mechanism and the information provided on International Data Transfers with Sentry to conduct your own due diligence on international data transfers with Sentry.

- ☐ **Select your data storage location**. Determine if you want to store your data in the EU, including to satisfy any internal compliance requirements.

4 ***Security of Processing*** *- Appropriate technical and organizational measures to ensure security of processing.*

How does Sentry meet GDPR obligations?

We build security into our product, perform rigorous testing, and implement security, privacy, and compliance controls set to global standards.

- Security Policy. Our Security Policy sets forth the steps we take to secure the Sentry service and our customers' service data.
- Penetration testing. We engage security consulting firms to complete regular penetration tests on the Sentry service. Results of our latest penetration tests are made available in the legal and compliance tab in your Sentry service settings.
- Compliance certifications. We engage third-party auditors to verify that compliance controls are operating effectively. Our latest SOC2 Type 2 report and ISO 27001 certificate are made available in the legal and compliance tab in your Sentry service settings.
- Security questionnaire. To enable our customers to assess our security controls, we've pre-populated a Consensus Assessment Initiative Questionnaire (CAIQ) developed by the Cloud Security Alliance, an independent research organization.

WHAT DO YOU NEED TO DO?

- ☐ **Evaluate level of security**.
  - ☐ Review Sentry security documentation.
  - ☐ Confirm the level of security provided is appropriate to the risk in relation to the data you configure to be sent to Sentry.
- ☐ **Manage login credentials**. Ensure login credentials are kept confidential, and not shared with others.
- ☐ **Manage your access points**. Secure the systems and devices you use to access Sentry.

5 ***Notices and Consents*** *— Provide notices or obtain consents necessary to engage third-party processors, such as Sentry*

How does Sentry meet GDPR obligations?

We disclose to you the third parties we engage to help us process your data (i.e., our subprocessors) and commit to notify you of any changes to such subprocessors, as required under GDPR. For certain Sentry services, this may require you to subscribe to our RSS feed, as set forth in our Data Processing Addendum.

WHAT DO YOU NEED TO DO?

You may have your own notice and consent obligations.

Consider whether you need to:

- ☐ **Notices**. Update your customer-facing disclosures to account for your use of Sentry
  - E.g., your subprocessor list, website or app privacy notice
- ☐ **Consents**. Obtain consents
  - E.g., opt-in consent for Sentry SDKs via your website or app consent banner

Your obligations depend on how you deploy Sentry, the local laws that apply to you, and the nature of your relationship with the EU individuals to which the data relates (e.g., direct or indirect).

6 ***Respond to Data Subject Requests*** *— Respond to requests from EU individuals to exercise their GDPR rights (e.g., delete, receive a copy of, or exercise other rights with respect to their personal data)*

How does Sentry meet GDPR obligations?

Sentry's responsibility is to assist you with any requests you may receive from EU individuals to exercise their GDPR rights with respect to any of their personal data incorporated in service data. We do so by:

- Forward requests. We will promptly forward any such requests that are received by Sentry.
- Include built-in functionalities. We provide you with built-in functionalities to manage your event data and respond to any such requests.

WHAT DO YOU NEED TO DO?

You are responsible for responding to data subject requests. This means you should:

- ☐ **Know your data.** Understand your Sentry configuration and where personal data may be captured (see Data Minimization above).
- ☐ **Respond to requests.** Action requests from EU individuals regarding their personal data, including by using Sentry's built-in functionalities.
  - ☐ Query your data - The data you send to Sentry is accessible via your Sentry interface, and Sentry has functionalities, such as Discover, that allow you to search for specific data..
  - ☐ Delete your data - Sentry also enables you to delete data. You can access these functionalities on the Sentry interface and via Sentry's API.

As used in this document, the EU refers to the European Union and GDPR refers to the General Data Protection Regulation (Regulation (EU) 2016/679). We also refer to GDPR terms such as "data subject", "personal data", "processor", "processing" (and its derivatives) and "transfer". Check out the definitions set forth in the GDPR.

This guidance is intended to be informative and highlight compliance areas you should consider. It is not intended to be legal advice. Ultimately, you should consult with your own legal counsel to determine the specific GDPR compliance obligations that apply to you and your business.

This document was created on March 11, 2024.

SENTRY