Data Security with Sentry

Data Encryption
Data in transit and at rest is encrypted using AES-256. Additional field-level encryption is applied to sensitive fields at rest.

Data Storage & Retention
Sentry is hosted on Google Cloud Platform, which is ISO27001 and SOC2 certified. Data is retained for 90 days. Sentry keeps hourly encrypted backups in multiple regions.

Data Controls
Sensitive data can be scrubbed before it is sent to or before it is stored on Sentry. In other words, you decide what data you want to send, process, and store.

Access management
Role-based access controls allow customers to provide the right Sentry access to specified team members. Single-Sign-On/SAML can be utilized to provide and regular access. In-app audit logs provide insights into user actions.

Security Testing
We seek out and proactively address vulnerabilities and exposures in Sentry's code and dependencies through automated tools, peer-review, penetration tests, and a public bug bounty program.

Single-Tenant

Sentry offers single-tenant instances of our platform for customers who require complete segregation of data and infrastructure.

Verified Security Practices

SOC2
Our security processes and controls are verified to meet SOC 2 security standards. SOC-2 Report can be sent upon request.

GDPR
As part of our GDPR compliance, Sentry provides a standard Data Processing Addendum (DPA) is found here: https://sentry.io/legal/dpa/1.0.0/.

HIPAA and HITECH
Sentry is HIPAA and HITECH compliant and Business Associate Agreements (BAA) are available to Enterprise customers.