Security & Compliance at Sama

IBM reported the average cost of a security data breach is $3.86 million, up 6.4 percent from last year. Our secure and compliant annotation platform and ISO certified delivery centers protect clients from costly mistakes that arise from poor security protocols.

Compliant Data Annotation

Platform Security

Following data security best practices, we protect your data from unauthorized access and data corruption throughout its lifecycle.

- Data storage encryption at transit and at rest
- Secure web and API communication
- Self generated client IDs maintain the anonymity of the client

Physical & Logical Security Requirements

Our priority is making sure your data is protected from ingestion to delivery. Delivery centers meet the most stringent physical and logical security requirements. They are equipped with biometric authentication for identification and access control, and our directly managed workforce delivers all work in ISO certified facilities.

Sama Security Measures

Data Residency	In-country legal compliance on items related to privacy, banking, government, and intellectual property protection.
Data Transit Protection	Communication between Sama clients and our servers is encrypted via industry-standard Transport Layer Security (TLS), TLS/SSL.
Limited Data Access	• Data only accessible to authorized personnel (POLP) • Access control per tenant with Amazon S3
Vulnerability Testing	• External pen-testing to further protect client assets from theft and unauthorized access. • White Hat automated security scanning
Secure Work Environment	• ISO Certified Delivery Centers • Biometric Authentication • User Authentication with 2FA