Data Privacy at Sama

At Sama, security and trust are our top priorities. We're committed to helping our clients comply with data privacy regulations like GDPR and CCPA and being your trusted training data strategy, annotation and validation partner.

The General Data Protection Regulation (GDPR) applies to any company that handles the personal data of residents in the Eurpoean Union (EU) and European Economic Area (EEA). Because Sama works with companies who serve customers in the EU and EEA, as well as clients based in the EU and EEA, the GDPR applies to our business.

The California Consumer Privacy Act (CCPA) is planned to go into effect on January 1, 2020. CCPA's primary purpose is to protect the personal information of persons domiciled in California, and as a company doing business in California, the CCPA also applies to our business.

Additionally, as a global enterprise that strongly supports data protection and privacy regulations, we offer clients the personal data protection rights, under the GDPR and CCPA, wherever they live.

How Sama Protects Your Personal Data

The GDPR separates data protection responsibilities into two categories: controllers and processors. Sama is GDPR compliant as a data processor and therefore adheres to all requirements related to the processing of personal data based on documented instructions from our clients.

The CCPA applies to any business collecting or storing data about California residents. Sama is CCPA compliant as a California based business and adheres to all requirements related to the processing of personal data for California residents.

PII, GDPR, and Security at Sama

Privacy and security are fundamental design requirements in our technologies, services, business practices and operations. We're dedicated to ensuring all the information you share with us is kept secure and that you're in control of who can access it.

Limitation of Purpose, Data and Storage	• Limited to Assets, APIs and manual request for data deletion • Strictly limited to material pertaining to the data annotation
Security	• Access control, physical and logical • Principle of least privilege • API access to tasks and assets deletion • Encryption • Security Training • Regular pen-testing
Operational Excellence	• Tier 1 service providers • Configuration Management • Logging and Triggering
Data Subject Requests and Receipt	• Via the customer • Identified by AssetID • Confirmation via access log
Privacy	• Data only accessible to Authorized personnel (POLP) • Sama self generated IDs
Notification	• Tier 1 cloud service providers • 72h incident response