How Continual Protects Your Data

Continual is trusted with the most sensitive customer information of leading organizations. Security, compliance, and privacy have been of utmost priority from day one. This white paper gives an overview of the measures we take to protect your data.

GDPR compliant

CCPA compliant

SOC 2 Type 2 compliant

Secure By Design

Continual's architecture is secure by design. Continual operates as a cloud software-as-a-service (SaaS) platform where all customer data remains stored on your company's cloud data warehouse. This hybrid architecture means Continual only accesses data during model training and prediction operations using credentials controlled fully by the customer. Data is never persisted on the Continual platform and Continual fully respects the underlying data warehouses security policies. Machine learning features and predictions generated by Continual are stored in your cloud data warehouse not in the Continual platform.

Built Using Secure Infrastructure

Continual runs on the Google Cloud Platform in an isolated production VPC and uses industry best practices to ensure a high level of physical, virtual, and network-level security that significantly reduces our security surface area. Continual also enables customer facing networking security options such as allowed IP addressing. Continual is operated in Google Cloud Platform's USA us-central1 region.

Data Encrypted in Transit & At-Rest

Continual's metadata database (Google Cloud SQL) is encrypted by Google Cloud Platform using AES-256 encryption or higher. All ingress and egress is encrypted via TLS 1.2+. Cryptographic tools operate in Google Cloud Platform's USA us-central1 region.

Access Control and User Auditing

For access to customer data warehouses, Continual requires user and role-based authentication to ensure minimum levels of permission necessary and creates full audit logs for every action taken. By avoiding data replication, Continual works seamlessly with the underlying data warehouse security policies, audit capabilities, and usage limits.

Access to the customer's cloud data warehouse is 100% controlled by the customer. By default, we recommend walling off the Continual service account so that it only has write access into a dedicated database and read access into relevant source tables. Customers can additionally choose to implement separate databases per project to further isolate work and ensure no sharing of data across projects.

Continual Follows Industry Best Practices

Continual uses enterprise-grade best practices to protect our customers' data, including automated and manual testing, code reviews, continuous deployments, production logging and alerts, and regular performance benchmarking. There is full logical separation of development and production environments, with named, dedicated accounts for each, and highly limited and audited access to production.

For questions or to see our DPA, reach out to us at

→ security@continual.ai