Security & Data Overview

Keystone — institutional risk & reporting infrastructure for digital-asset funds

DATA RESIDENCY

All data processing occurs within the European Union.

A single encrypted EU datastore holds all application data. No third-party object storage.

CONTROLS

Data residency
All data is processed and stored within the European Union, on established cloud infrastructure.

Read-only connectivity
Venue and custodian connections use read-only API credentials. Keystone never requests withdrawal, transfer, or trading permissions.

Encryption
Encrypted in transit (TLS) and at rest (AES-256), across compute and storage.

Credential handling
Connection credentials are encrypted at rest and held in a dedicated secrets vault, never in source code.

Access control
Role-based access: administrator, viewer, and auditor roles, over authenticated sessions.

Infrastructure security
Administrative access is protected with two-factor authentication; deployments use federated identity with no long-lived keys.

Audit & evidence
Risk-state transitions are recorded in an append-only audit trail, with evidence bundles attached to report outputs.

Data footprint
All application data resides in a single encrypted EU datastore. No third-party object storage.

ACCESS MODEL

Administrator
Manages configuration and access.

Viewer
Reads risk state and reports.

Auditor
Reviews the audit trail and evidence.

READ-ONLY POSTURE

Read-only	Keystone observes and reports. It does not place, modify or route orders.
No custody	It never holds assets, keys or client funds. Positions are read, never controlled.
No trading permissions	Venue and custodian credentials are read-only. No withdrawal, transfer or trading scope is requested.