

SECURITY AND TRANSPARENCY

How we secure your data

A companion to the OakQuant Privacy Policy. Understand the controls, processing boundaries, and limits.

Last updated: 2026-10-31 · Version 2026-10-31 · Operated by Revelar Inc.

1. Who is responsible and what this covers

Revelar Inc. operates OakQuant, its platform name. This policy covers the OakQuant Investing website and app, Acorn, and related newsletter records. Contact admin@oakquant.ai for privacy questions, account requests, or security concerns. Linked products and third-party providers may have separate policies.

This policy explains service data use. It is not a promise of absolute security or a claim that all processing stays on your device. Services and AI providers may process information outside your state or country, including in the United States, where privacy laws may differ.

4. AI processing and explainability

When you request an AI feature, relevant parts of your prompt and service context may be sent to an external AI provider to generate the response. This can include financial information if your request uses holdings or goals. The service uses input minimization where integrated, but you should not assume that personal information is removed or that every request is anonymous.

Provider handling, retention, and any model-training eligibility depend on the provider, endpoint, and contract used for that feature. This policy does not promise zero retention, local-only processing, or exclusion from provider training across every feature. Contact us before submitting information if you need those guarantees.

AI can produce incorrect statements, incomplete sources, or misleading confidence. Ask for the source, observation date, assumptions, missing inputs, and method behind a result. Where a source or evidence is unavailable, treat the conclusion as unverified. An explanation is not a guarantee that a model's reasoning is complete or accurate.

How a research request uses data

External AI processing may receive relevant financial context.

01

Your request

You supply a question and relevant context.

02

Service processing

Authorized tools retrieve and organize information.

03

AI, when needed

An external provider may process selected context.

04

Your review

Check sources, dates, assumptions, and risks.

Illustration of the security design and processing boundaries. No system guarantees absolute security.

6. How we secure your data

Our security design uses HTTPS for public service connections, authenticated service access, signed access tokens, and user and organization permissions to restrict access. These controls address different risks: protecting information in transit, establishing identity, and limiting what an identity may read or change.

Operational credentials are managed separately through a secrets service and injected at runtime. They are not intended to be included in prompts or user-facing files. Access controls and data minimization reduce exposure; they do not eliminate every risk.

We do not claim end-to-end encryption, universal encryption of every stored field, independent security certification, or immunity from breaches. If a security incident triggers notification duties, we will notify affected people or authorities as required by law. Protect your own credentials and report suspected misuse promptly.

How we secure your data

Different controls address different risks.

01

Encrypted connection

Public HTTPS connections protect data in transit.

02

Authenticated identity

Access tokens identify the requesting account.

03

Scoped access

Permissions restrict access to user and workspace data.

04

Separate secrets

Operational credentials stay outside product content.

Illustration of the security design and processing boundaries. No system guarantees absolute security.

7. Retention and deletion

Retention depends on the record and its purpose. Account data, saved research, workflow history, and preferences may remain while needed to provide the service. Security, billing, consent, and dispute records may need to be retained for legal, fraud-prevention, or operational reasons. This policy does not state a single retention period for every category.

You may request deletion or account closure. We verify authority before disclosing or deleting personal data. Deletion may be subject to legal exceptions, backup lifecycles, and separate provider follow-up. Unsubscribing stops future subscribed messages; it does not erase every record. Previously delivered email or content copied by other people cannot be recalled by deleting an OakQuant record.

8. Your rights and choices

Depending on your location, you may have rights to access, correct, export, or delete personal data; restrict or object to processing; withdraw consent; or complain to a privacy regulator. Contact admin@oakquant.ai with your request and location. We will verify your identity proportionately and respond as required by applicable law. Do not email passwords or full financial account numbers.

Use newsletter unsubscribe links to stop subscribed mail. The newsletter privacy page supports verified export or erasure requests for newsletter records. Account-wide requests are separate. Disconnect linked accounts through the relevant integration or provider; disconnecting does not automatically delete historical records.

Browser storage is used for functions such as sessions, theme choices, and preferences. Clearing it may sign you out or reset preferences. Third-party pages and embeds have their own storage practices. Browser privacy controls do not automatically close an account or revoke a third-party connection.

Current online version: oakquant.ai/privacy#security