

YOUR DATA, EXPLAINED

Privacy Policy

What we collect, why we use it, where AI fits, and how to exercise your choices.

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.

2. Information we collect

Account and organization data: information you provide when registering or updating a profile, such as name, email, preferences, organization membership, and permissions. Authentication and security records support account access and abuse prevention.

Financial and workflow data: goals, holdings, transactions, watchlists, assessment answers, research requests, files, and other information you enter or authorize a connected provider to supply. The categories available depend on the feature and the permissions you grant. Do not enter account passwords or unnecessary identifiers in chat.

Interaction and technical data: prompts, responses, workflow results, feedback, support requests, consent and subscription records, and technical records such as request times, device or browser information, IP addresses, and errors when collected by the service or its infrastructure. These records can include personal information.

Newsletter data: email address, selected topics, confirmation and unsubscribe records, and delivery information supplied by the email provider. A newsletter subscription does not require an Investing account.

3. Why and how we use information

We use information to create and authenticate accounts, enforce organization permissions, run requested research and workflows, maintain connected-account features, provide support, deliver subscribed messages, process billing through payment providers, and investigate security or reliability issues.

Saved outcomes and feedback can be used to evaluate forecasts and improve service behavior. That is distinct from training a third-party language model. A forecast adapting to measured outcomes is not evidence of investment performance.

Where applicable law requires a legal basis, processing may be necessary to provide a requested service, comply with legal obligations, pursue legitimate interests such as service security and reliability, or act on consent for optional features and communications. You may withdraw consent for future optional processing without affecting earlier lawful processing.

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.

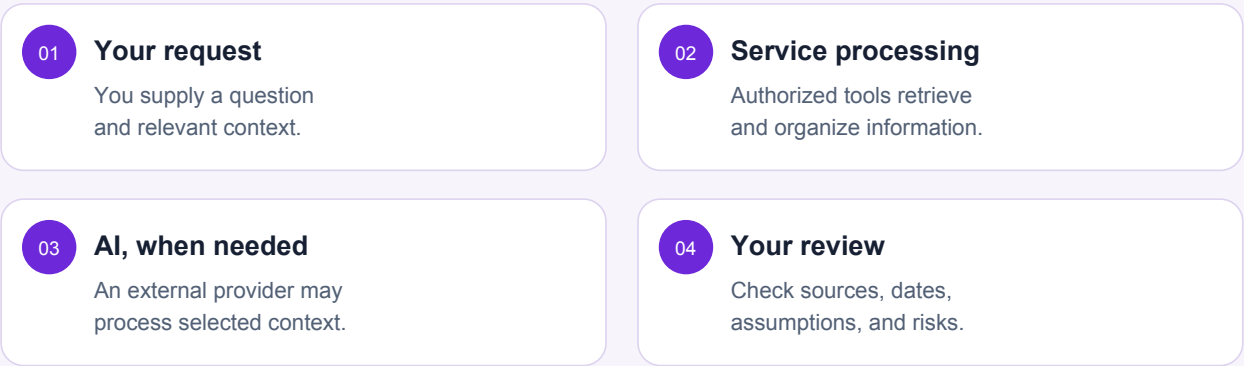


Illustration of the security design and processing boundaries. No system guarantees absolute security.

5. Who may receive data

Service providers may receive the information needed for hosting, storage, AI processing, connected-account access, payments, email delivery, and support. Examples of integrations include Plaid for account connections, Stripe for payments, and Resend for newsletter delivery, where enabled. Each provider’s own handling is governed by its applicable terms and our service arrangements.

Organization administrators and authorized reviewers may access records within the permissions of your workspace. Review your organization’s arrangements before entering sensitive information. Content you choose to publish or share may become visible to its selected audience or the public.

We may disclose information when required by law, to protect rights or safety, investigate fraud or abuse, or as part of a business transfer subject to applicable protections. Ask us about the recipient and purpose of a specific disclosure before submitting information if you need a restricted processing arrangement.

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.

9. Children and policy changes

The Investing service is intended for adults, not children under 18. If you believe a child has submitted personal information, contact us so we can investigate and handle it appropriately.

The version date identifies this policy. We will provide appropriate notice of material changes and obtain consent when required. Contact admin@oakquant.ai if you need clarification about a feature or this policy.

Current online version: oakquant.ai/privacy