Data Processing Agreement (DPA)

QuantRidge — B2B processing agreement (GDPR Article 28–style template)

Effective date: March 29, 2026
Version: 1.0

---

1. Parties

This Data Processing Agreement ("**Agreement**") is entered into between:

1. **Customer** — the legal entity that has entered into an order, subscription, or other contract with QuantRidge for use of the Services (the "**Controller**" or "**Customer**" where it determines the purposes and means of processing of personal data, or acts as an independent controller where applicable under applicable law); and
2. **QuantRidge** ("**Processor**," "**we**," or "**us**") — the provider of the QuantRidge platform and related services described below.

This Agreement supplements the main agreement between the parties ("**Principal Agreement**"). If there is a conflict regarding data protection obligations, the stricter or more specific requirement applies, unless the Principal Agreement expressly states otherwise for a signed enterprise order.

---

2. Definitions

Capitalized terms not defined here have the meanings in the Principal Agreement or in applicable data protection law (including the EU General Data Protection Regulation, "**GDPR**," and the UK GDPR as applicable).

- **Personal Data** — any information relating to an identified or identifiable natural person processed by Processor on behalf of Customer in connection with the Services.
- **Processing** — any operation or set of operations performed on Personal Data (including collection, storage, use, disclosure, and deletion).
- **Subprocessor** — a third party engaged by Processor to process Personal Data in connection with the Services.
- **Services** — as defined in Section 3.

---

3. Description of processing

3.1 Subject matter and duration

The subject matter is Processor's provision of the Services to Customer. Processing continues for the term of the Principal Agreement and until Personal Data is returned or deleted in accordance with this Agreement and the Principal Agreement, unless a longer retention period is required by law.

3.2 Nature and purpose of processing

Processor processes Personal Data to:

- Provide, operate, secure, and improve the QuantRidge **application** (hosted application and APIs) and the **public website**;
- Authenticate users, manage accounts, workspaces, and permissions;

- Deliver financial modeling, analytics, reporting, and related product features;
- Provide **AI-assisted features** where enabled (including interactions sent to third-party model providers as described in the Privacy Policy);
- Operate **integrations** Customer enables (e.g., market data, connectivity, or payments providers);
- Process **billing and subscriptions**;
- Provide **customer support**, service communications, and optional marketing in line with Customer's marketing preferences where applicable;
- Maintain **logs, monitoring, and security** (including fraud and abuse prevention);
- Comply with **legal obligations** and enforce terms.

3.3 Types of Personal Data (illustrative)

Depending on how Customer uses the Services, this may include:

- **Identifiers and contact data:** name, email address, account identifiers, company affiliation;
- **Authentication data:** session tokens, credentials metadata (passwords are not stored in plain text);
- **Usage and technical data:** IP address, device/browser data, logs, feature usage;
- **Content Customer uploads** into the platform (which may include Personal Data about data subjects Customer chooses to analyze);
- **Payment-related data** as handled by payment service providers (Processor generally receives limited billing metadata, not full card numbers, depending on integration).

3.4 Categories of data subjects

Customer's personnel and authorized users; individuals whose Personal Data appears in content Customer uploads or connects through integrations; and other categories Customer instructs via use of the Services.

3.5 Role of the parties

For Personal Data that Customer (or Customer's organization) controls under applicable law, **Customer is the controller** (or processor to its own customers, as the case may be) and **QuantRidge is the processor**, except where both parties act as **independent controllers** for distinct purposes (e.g., certain account, billing, or security activities), in which case each party complies with its own obligations under applicable law. Nothing in this Agreement is intended to reduce Customer's obligations to its own end users or employees.

---

4. Customer instructions

Processor will process Personal Data only:

- On documented instructions from Customer, including as set out in this Agreement and the Principal Agreement; and
- As required by applicable law (in which case Processor will inform Customer of that legal requirement before processing, unless prohibited by law).

Customer instructs Processor to process Personal Data as reasonably necessary to provide the Services and as otherwise configured by Customer through the product (e.g., enabled integrations, invited users, uploaded content).

---

5. Processor personnel and confidentiality

Processor ensures that persons authorized to process Personal Data are bound by appropriate confidentiality obligations (contractual or statutory).

---

6. Security measures

Processor implements appropriate technical and organizational measures appropriate to the risk, including, where applicable:

- **Encryption in transit** (e.g., TLS) for data transmitted over public networks;
- **Encryption at rest** relying on industry-standard capabilities of hosting and database providers;
- **Access controls** and authentication for production systems;
- **Logical separation** of Customer data within multi-tenant architecture where applicable;
- **Logging and monitoring** for security and reliability;
- **Incident response** procedures designed to detect and respond to security incidents.

Customer is responsible for maintaining the security of its accounts (e.g., strong passwords, MFA where offered) and for the lawfulness of data it uploads or connects.

---

7. Subprocessors

7.1 Authorization

Customer generally authorizes Processor to engage **Subprocessors** listed or described in Processor's **Privacy Policy** and subprocessors disclosures on the website, and to engage additional or replacement Subprocessors in accordance with Section 7.3.

7.2 Current Subprocessors (illustrative — March 2026)

The following categories and named providers reflect typical subprocessors. **The authoritative list** for objections and updates is maintained in Processor's **Privacy Policy** / security pages and internal vendor records. Update this table when vendors change.

Subprocessor (category / name)	Role
Render	Application hosting, managed PostgreSQL, related infrastructure
Vercel	Frontend / edge hosting (where used)
Stack Auth / Supabase Auth	Authentication and identity services
OpenAI, Groq, and other LLM APIs	AI features and model inference (content sent per product configuration)
Plaid, Stripe, SnapTrade, Finnhub (and similar)	Payments, financial account linking, and market data integrations **when Customer enables them**

Processor imposes data protection terms on Subprocessors that process Personal Data, consistent with Article 28(4) GDPR where applicable.

7.3 Changes and objection

Processor will publish updates to Subprocessors (e.g., via the Privacy Policy or a subprocessors page). If Customer has a **reasonable, documented objection** to a new Subprocessor on **material data protection grounds**, Customer may notify Processor within **thirty (30) days** of the change. The parties will work in good faith to resolve the objection (which may include alternative configuration, cessation of use of a non-essential feature, or termination of affected Services if no alternative is feasible).

---

8. International transfers

Where Personal Data originating from the **EEA**, **UK**, or **Switzerland** is transferred to countries not recognized as providing adequate protection, Processor will implement appropriate safeguards, such as the **EU Standard Contractual Clauses** (and UK Addendum where applicable), or another lawful transfer mechanism. Details may be provided upon request or as referenced in the Privacy Policy.

---

9. Assistance to Customer

Taking into account the nature of processing, Processor will assist Customer, by appropriate technical and organizational measures where reasonably possible, with:

- **Data subject requests** (access, deletion, correction, etc.) — Customer may route requests through **support@quantridge.net** and in-product tools where available;
- **Data protection impact assessments** and prior consultation with supervisory authorities, where required and to the extent Processor's assistance relates to the Services;
- **Security incidents:** Processor will notify Customer **without undue delay** after becoming aware of a **personal data breach** affecting Customer's Personal Data, and will provide information reasonably necessary for Customer to meet its breach notification duties, where such information is available.

---

10. Return and deletion

Upon termination or expiry of the Services (or upon Customer's written request, where agreed), Processor will **delete or return** Personal Data in accordance with the Principal Agreement and product capabilities, except where retention is required by law or for legitimate backup/disaster recovery for a limited period, after which deletion will occur.

---

11. Audits and information

Processor will make available information reasonably necessary to demonstrate compliance with Article 28 GDPR and will allow for and contribute to **audits**, including **inspections**, conducted by Customer or an auditor mandated by Customer, **subject to:** (a) reasonable notice; (b) frequency limits (e.g., not more than once per year except for a genuine suspected breach); (c) confidentiality; and (d) substitution with a third-party certification or audit report where appropriate and commercially reasonable.

---

12. Liability

Liability for breaches of this Agreement follows the liability provisions of the Principal Agreement, subject to mandatory applicable law.

---

13. Order of precedence

If this Agreement conflicts with the Principal Agreement solely with respect to **data protection**, the terms of this Agreement prevail. For all other matters, the Principal Agreement prevails.

---

14. Contact

QuantRidge — privacy and DPA inquiries: **support@quantridge.net**

---

15. Important notice (template disclaimer)

This document is a **business and legal template** for negotiation and execution between QuantRidge and its business customers. **It is not legal advice.** Customer should have **qualified counsel** review this Agreement together with the Principal Agreement, order form, and applicable privacy laws before execution.

End of document