Data Processing Agreement

Last updated: 16 September 2026 · [Operating entity, registered address & governing law — to confirm before launch]

1. Parties and roles

This agreement is between you (the "Customer") and QuanticData ([Operating entity, registered address & governing law — to confirm before launch]). For **account, billing and usage data**, the Customer is the controller and QuanticData is the processor. For **data the Customer collects through the service** — pages, search results, datasets — the Customer is the controller and decides what is collected; QuanticData processes it only to deliver the result requested.

2. Subject matter and duration

Processing lasts for the term of the Customer's account and consists of operating the proxy networks, APIs and dashboard described in the Terms. On termination, see section 8.

3. Categories of data and data subjects

- **Customer personnel**: name, email address, hashed password or SSO identity, IP address, user agent, phone number when verified, invoice records and the last four digits of a card.
- **Usage records**: endpoints called, timestamps, outcome, latency, cost, target host.
- **Content retrieved on the Customer's instruction**, which may contain personal data chosen by the Customer. We do not select it, mine it, or retain it beyond delivery of the result.

4. Our obligations

- Process personal data only on the Customer's documented instructions, including for transfers, unless law requires otherwise — in which case we tell the Customer first unless prohibited.
- Bind everyone with access to confidentiality.
- Implement the technical and organisational measures in section 5.
- Assist the Customer with data-subject requests, DPIAs and consultations, to the extent the data is in our systems.
- Make available the information needed to demonstrate compliance, and allow audits as set out in section 9.

5. Security measures

- **In transit**: TLS on every public endpoint, HSTS on our sites; proxy credentials are per-account and revocable.
- **At rest**: passwords stored as salted hashes, API keys stored hashed or encrypted, support attachments stored outside the web root and served only through signed, expiring links.
- **Access control**: role-based access to the admin surface, individual named accounts, no shared logins, MFA available on customer accounts and used internally.
- **Segregation and hosting**: production runs in the EU (Frankfurt) on dedicated infrastructure; releases are deployed blue/green with the previous version kept for rollback.
- **Logging and monitoring**: request and admin action logs, rate limiting, automated abuse and fraud guards, alerting on anomalies.
- **Data minimisation**: we do not retain fetched page content beyond what is needed to return a result, and analytics runs on EU infrastructure.

We do not currently hold ISO 27001 or SOC 2 certification and we do not claim it. The measures above are what we actually operate; we will describe any of them in more detail on request.

6. Sub-processors

A current list of sub-processors, with purpose and location, is provided to customers under a DPA on request — write to privacy@quanticdata.io. We impose data-protection obligations on each of them no less protective than this DPA, and we remain liable for their performance. We give at least 14 days' notice by email before a new sub-processor starts processing personal data; the Customer may object on reasonable data-protection grounds and, if we cannot resolve the objection, may terminate the affected service.

7. International transfers

Production data is hosted in the EU. Where a sub-processor processes personal data outside the EEA, the transfer relies on an adequacy decision where one applies, and otherwise on the European Commission's Standard Contractual Clauses (module two, controller to processor), which are incorporated into this DPA by reference, together with supplementary measures where required.

8. Return and deletion

On termination, or on written request, we delete or return personal data processed on the Customer's behalf. Account and usage records are deleted within 30 days of account closure, except where retention is required by law (for example invoices, which tax law requires us to keep). Backups are overwritten on their normal cycle, within 90 days.

9. Audit

We answer security questionnaires and provide documentation of the measures in section 5. A Customer under a DPA may audit, or appoint an independent auditor, once in any 12-month period on 30 days' notice, during business hours, without disrupting the service and subject to confidentiality; more often if a supervisory authority requires it.

10. Personal data breach

We notify the Customer **without undue delay and in any event within 72 hours** of becoming aware of a personal data breach affecting their data, with the information available at the time — what happened, which data and how many records are involved, the likely consequences and the measures taken — and we follow up as the picture becomes clearer.

11. Order of precedence

In case of conflict, this DPA prevails over the Terms of Service for matters of personal data processing. Everything else in the Terms continues to apply.

Questions, a countersigned copy, or your own DPA paper: privacy@quanticdata.io.
