Data Processing Agreement

Between Customer ("Controller") and Queri LLC ("Processor")

Version 1.0 — Effective March 2026

This Data Processing Agreement ("DPA") forms part of the agreement between the entity identified below ("Customer" or "Controller") and Queri LLC, a company incorporated in Idaho, United States ("queri" or "Processor"), for the provision of the queri platform and services ("Services").

This DPA sets out the terms that apply when Personal Data is processed by queri on behalf of Customer in the course of providing the Services. The purpose of this DPA is to ensure compliance with Article 28 of the General Data Protection Regulation (EU) 2016/679 ("GDPR"), the California Consumer Privacy Act ("CCPA"), and other applicable data protection laws.

1. Definitions

"Personal Data" means any information relating to an identified or identifiable natural person that is processed by the Processor on behalf of the Controller in connection with the Services.

"Processing" means any operation performed on Personal Data, including collection, recording, organization, storage, retrieval, use, disclosure, erasure, or destruction.

"Sub-Processor" means any third party engaged by the Processor to process Personal Data on behalf of the Controller.

"Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data.

"Services" means the queri AI-powered knowledge management platform, including document indexing, semantic search, chat-based knowledge retrieval, and related functionality.

2. Scope and Purpose of Processing

The Processor shall process Personal Data solely for the purpose of providing the Services as described in the Agreement between the parties. Specifically, the Processor processes documents, meeting transcripts, support tickets, chat messages, and other content connected by the Customer to provide AI-powered search and knowledge management.

2.1 Categories of Personal Data

- Employee names, email addresses, and job titles
- Meeting attendee lists and calendar data
- Customer/client names and contact information contained in support tickets
- Any other personally identifiable information contained within documents, messages, or files connected by the Customer to the Services

2.2 Categories of Data Subjects

- Customer's employees and contractors
- Customer's clients and their employees (for agencies and consulting firms)
- End-users of Customer's products and services (for SaaS companies)

2.3 Duration of Processing

Personal Data shall be processed for the duration of the Agreement. Upon termination of the Agreement or upon Customer's request, the Processor shall delete all Personal Data within thirty (30) days. Backup copies shall be deleted within an additional thirty (30) days.

3. Obligations of the Processor

The Processor shall:

- Process Personal Data only on documented instructions from the Controller, unless required by applicable law;
- Ensure that persons authorized to process Personal Data are bound by confidentiality obligations;
- Implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk (see Section 5);

- Assist the Controller in responding to requests from data subjects exercising their rights under applicable data protection law;
- Assist the Controller in ensuring compliance with obligations related to security, breach notification, impact assessments, and consultation with supervisory authorities;
- At the Controller's election, delete or return all Personal Data upon termination of the Agreement;
- Make available to the Controller all information necessary to demonstrate compliance with this DPA.

4. Sub-Processors

The Controller provides general authorization for the Processor to engage Sub-Processors for the processing of Personal Data. The current list of Sub-Processors is maintained at **queri.so/legal/sub-processors** and is incorporated by reference into this DPA.

The Processor shall:

- Notify the Controller at least thirty (30) days before adding or replacing a Sub-Processor;
- Impose on each Sub-Processor data protection obligations at least as protective as those in this DPA;
- Remain fully liable to the Controller for the performance of each Sub-Processor's obligations.

If the Controller objects to a new Sub-Processor within the notification period, the parties shall discuss the Controller's concerns in good faith. If the objection cannot be resolved, the Controller may terminate the affected Services.

5. Security Measures

The Processor shall implement and maintain the following technical and organizational security measures:

MEASURE	IMPLEMENTATION
Encryption at rest	AES-256 encryption for all stored data

Encryption in transit	TLS 1.2+ for all data transmission
Data isolation	Row-Level Security (RLS) per organization; no cross-tenant data access
Access controls	Role-based access control (RBAC) with admin and member roles
Authentication	Secure session management via Supabase Auth; SSO/SAML on eligible plans
Audit logging	Administrative actions logged with user, timestamp, and action
Application security	Security headers (CSP, HSTS), rate limiting, input validation, SAST scanning
Dependency monitoring	Automated vulnerability scanning of dependencies
Infrastructure	SOC 2 Type II certified hosting (Vercel, Supabase/AWS); see Sub-Processor list

6. Data Breach Notification

In the event of a Data Breach affecting Personal Data processed under this DPA, the Processor shall:

- Notify the Controller without undue delay, and in any event within seventy-two (72) hours of becoming aware of the breach, consistent with GDPR Article 33;
- Provide sufficient information to allow the Controller to meet its own notification obligations;
- Take reasonable steps to mitigate the effects of the breach and to prevent further breaches;
- Cooperate with the Controller in investigating and remediating the breach.

7. Data Subject Rights

The Processor shall assist the Controller in responding to requests from data subjects exercising their rights under applicable data protection law, including rights of access, rectification, erasure, data portability, restriction of processing, and objection to processing.

Upon receiving a data subject request directly, the Processor shall promptly redirect the request to the Controller unless otherwise instructed. Deletion of data subject information across all systems, including vector embeddings, shall be completed within thirty (30) days of a validated request.

8. International Data Transfers

All primary data processing occurs in the United States (Supabase/AWS us-east-1, Vercel US regions). For transfers of Personal Data from the European Economic Area, United Kingdom, or Switzerland to the United States, the parties agree to the EU Standard Contractual Clauses (SCCs) as set forth in Commission Implementing Decision (EU) 2021/914, which are incorporated by reference into this DPA.

Where the Controller is established in the EEA, the Controller is the "data exporter" and the Processor is the "data importer" for purposes of the SCCs.

9. AI-Specific Data Processing Provisions

The following provisions apply specifically to the Processor's use of artificial intelligence and machine learning technologies in providing the Services:

> ### 9.1 NO MODEL TRAINING
>
> Processor shall not use, and shall ensure its Sub-Processors do not use, Customer Data to train, fine-tune, retrain, or otherwise improve any machine learning model, artificial intelligence system, or algorithm, whether directly or indirectly. Customer Data is processed solely for the purpose of providing the Services as described in the Agreement.

> ### 9.2 LLM DATA HANDLING

When Customer Data is transmitted to third-party large language model providers (e.g., OpenAI, Anthropic) for inference, such data is: (a) transmitted via encrypted API calls, (b) processed in real-time for the sole purpose of generating responses, (c) not stored, cached, or retained by the LLM provider beyond the duration of the API request, and (d) subject to the LLM provider's zero-retention API terms. Processor maintains zero-retention agreements with all LLM Sub-Processors.

9.3 EMBEDDING STORAGE

Document content is processed into vector embeddings (numerical representations) stored in Processor's database for the purpose of semantic search. These embeddings cannot be reverse-engineered into the original text. Original document text is stored in chunked form alongside embeddings for citation purposes, subject to the same security measures and data isolation as all other Customer Data.

9.4 BRING YOUR OWN KEY (BYOK)

On eligible plans, Customer may provide their own API keys for LLM providers ("BYOK"). When BYOK is enabled, Customer Data transmitted to LLM providers is governed by Customer's direct agreement with the LLM provider. Processor is not a party to such agreements and assumes no liability for the LLM provider's handling of data in BYOK mode.

10. Audit Rights

The Controller may request that the Processor provide information necessary to demonstrate compliance with this DPA. With reasonable advance notice and during normal business hours, the Controller may audit the Processor's compliance with this DPA, subject to reasonable confidentiality obligations.

The Processor shall make available its SOC 2 Type II report (when obtained) and other relevant security documentation upon request.

11. Return and Deletion of Data

Upon termination of the Agreement:

- Customer may export all data in JSON/CSV format via the platform's export functionality;
- After export, or after a thirty (30) day grace period if no export is initiated, the Processor shall permanently delete all Customer Data from its systems;
- Backup copies shall be deleted within an additional thirty (30) days;
- The Processor shall certify deletion in writing upon Customer's request.

12. Governing Law

This DPA shall be governed by the laws of the State of Idaho, United States, without regard to its conflicts of law provisions, except to the extent that applicable data protection law requires otherwise.

13. Term

This DPA shall remain in effect for the duration of the Agreement and shall automatically terminate upon termination of the Agreement, subject to the Processor's obligation to delete Personal Data as set forth in Section 11.

Signatures

By signing below, the parties agree to the terms of this Data Processing Agreement.

DATA PROCESSOR — Queri LLC	**DATA CONTROLLER — Customer**
Matt Newbill Name	Name
CEO & Founder Title	Title
March 2026 Date	Date

Queri LLC · Boise, Idaho · queri.so · legal@queri.so
Sub-Processor List: queri.so/legal/sub-processors