SABERRA

Data Processing Agreement

Delaware Public Benefit Corporation

Standard Processor Agreement | Version 1.0 | Governed by the Laws of the State of Delaware

This Data Processing Agreement ("DPA") is entered into between the parties identified below and supplements the Saberra Services Agreement between them. In the event of conflict between this DPA and the Services Agreement, this DPA prevails with respect to data protection matters.

Data Controller	The client organization named in the Saberra Services Agreement ("Controller")
Data Processor	Saberra, a Delaware Public Benefit Corporation, providing the Saberra institutional memory platform ("Processor")
Effective Date	Date of the Services Agreement between the parties, or date of separate execution if signed independently

1. Definitions

In this DPA, the following terms have the meanings assigned below:

- Personal Data means any information relating to an identified or identifiable natural person (data subject), as defined under applicable privacy and data protection law.
- Processing means any operation performed on Personal Data, including collection, storage, use, transmission, or deletion.
- Sub-processor means any third party engaged by the Processor to carry out processing on behalf of the Controller.
- Canon means approved, human-reviewed institutional memory records stored in the Controller's Notion workspace.
- Candidate Record means an AI-generated draft record awaiting human review -- not yet Canon and not surfaced in query responses.
- Applicable Law means all federal, state, and local privacy, data protection, and security laws and regulations applicable to the processing of Personal Data under this DPA, including without limitation the Delaware Personal Data Privacy Act (DPDPA) and any other applicable US state privacy laws.

2. Scope and Purpose of Processing

The Processor shall process Personal Data solely to provide the Saberra institutional memory service as described in the Services Agreement and the companion Technical & Governance Documentation.

2.1 Nature of Processing

- Ingestion of email and meeting content from the Controller's designated capture inbox
- AI-assisted extraction of structured Candidate Records (decisions, tasks, risks, roles, policies)

- Storage of Candidate and approved Canon records in the Controller's Notion workspace
- Retrieval and natural-language Q&A over approved Canon records via Sera API

2.2 Purpose

To help the Controller preserve, structure, and retrieve institutional governance and operational memory. Processing is strictly limited to this purpose and shall not be used for any other purpose without the Controller's prior written consent.

2.3 Categories of Data Subjects

- The Controller's staff, leadership, and governance participants whose names, roles, decisions, or communications appear in ingested content
- External parties (partners, vendors, advisors) whose names or commitments appear in ingested content

Saberra's intended scope does not include student Personal Data. Processing of any student data requires a separate written amendment to this DPA executed by both parties.

2.4 Types of Personal Data

Names, email addresses, role titles, and statements made in meetings or correspondence as they appear in governance and operational content submitted by the Controller. The Controller is solely responsible for ensuring that content submitted to the capture inbox does not include Personal Data categories not covered by this DPA.

3. Controller Obligations

- The Controller is responsible for determining what content is submitted to the Saberra capture inbox.
- The Controller warrants that it has a lawful basis under Applicable Law for processing any Personal Data submitted to Saberra.
- The Controller is responsible for ensuring that student Personal Data, health data, and other sensitive special categories are not submitted to the capture inbox unless separately agreed in writing.
- The Controller maintains ownership of and full responsibility for all records stored in their Notion workspace.
- The Controller is responsible for configuring Notion workspace permissions to ensure appropriate access controls over their institutional data.

4. Processor Obligations

The Processor shall:

- Process Personal Data only on documented instructions from the Controller and only for the purposes set out in this DPA;
- Ensure all persons authorized to process Personal Data on its behalf are bound by appropriate confidentiality obligations;
- Implement the technical and organizational security measures described in Section 6;
- Not engage or replace Sub-processors without providing prior written notice to the Controller (see Section 5);
- Assist the Controller in responding to data subject rights requests under Applicable Law to the extent technically feasible;
- Notify the Controller of any Personal Data breach without undue delay and within 72 hours of becoming aware of it;
- Upon termination of the Services Agreement, delete or return all Personal Data to the Controller at the Controller's election within five (5) business days; and
- Make available to the Controller all information reasonably necessary to demonstrate compliance with this DPA and to facilitate audits as described in Section 11.

5. Sub-processors

The Processor engages the following Sub-processors, each of whom processes Personal Data as part of delivering the Saberra service. The Controller hereby provides general authorization for the use of Sub-processors listed in this Section, subject to the Processor notifying the Controller of any intended changes.

Sub-processor	Role	Nature of Processing	Data Location
Notion Labs, Inc.	Primary data storage	All extracted and approved records stored in the Controller's own Notion workspace. Subject to Controller's own Notion subscription terms.	United States (with data residency options)
Anthropic, PBC	AI extraction	Email and meeting text sent to Anthropic Claude API for structured extraction. Processing is transient -- Anthropic does not retain or train on API customer data under its standard usage policy.	United States (transient only)
Railway, Inc.	Cloud infrastructure	Saberra's services run on Railway infrastructure. Each client has a dedicated Railway project with isolated environment variables and database.	United States
Google, LLC	Meeting asset access & outbound email	Google Drive/Docs access via OAuth2 to retrieve meeting transcripts and recordings; Gmail API for outbound system notifications only.	United States / global CDN

The Processor will provide the Controller with at least thirty (30) days' prior written notice of any intended addition or replacement of a Sub-processor. The Controller may object within fifteen (15) days; if the parties cannot resolve the objection in good faith, the Controller may terminate the Services Agreement without penalty.

6. Technical and Organizational Security Measures

The Processor maintains the following measures throughout the term of this DPA:

- Encryption in transit: all data transmitted between services encrypted via TLS 1.2 or higher;
- Credential isolation: all API keys and credentials stored as environment variables; never committed to source code or application logs;
- Sensitive content gate: Personal Data, financial data, legal documents, and personnel matters are automatically flagged and routed to a restricted, admin-only review queue before any further processing;
- Human review gate: no AI-extracted content becomes searchable Canon without an explicit human approval action -- this constraint is enforced at the architectural level;

- Audit trail: every ingestion event recorded in a Processing Events database with timestamp, source email ID, and processing outcome;
- Crash-safe ingestion: messages are not marked processed until all processing steps complete; Notion deduplication on Message ID prevents double-processing on retry;
- Client-controlled revocation: removing the Notion integration token immediately and completely terminates all Processor access to the Controller's data;
- Dedicated environment: each client runs in an isolated cloud project with separate credentials, database, and environment variables, providing logical separation from other clients.

7. Data Subject Rights

Under Applicable Law, data subjects may have rights of access, correction, deletion, portability, and opt-out of certain processing. The Controller is the primary party responsible for responding to data subject rights requests.

The Processor will, upon written request from the Controller, within ten (10) business days of receiving a complete written request:

- Provide information about what Personal Data relating to an identified data subject is present in the Controller's Notion workspace;
- Delete Personal Data relating to a specific data subject from Candidate Records and Canon records, to the extent technically feasible; and
- Provide an export of records relating to a specific data subject in machine-readable format.

8. Data Transfers

The Processor is incorporated in Delaware, United States, and all Sub-processors are based in the United States. Processing under this DPA occurs within the United States. Where the Controller is located outside the United States, the Controller is responsible for ensuring that any cross-border transfer of Personal Data to Saberra is conducted in compliance with Applicable Law in the Controller's jurisdiction and for obtaining any required consents or authorizations for such transfers.

For Controllers operating in jurisdictions with active data protection regimes (including but not limited to the EU/EEA, UK, Canada, Costa Rica, and Latin American jurisdictions with national data protection laws), the parties agree to execute any additional transfer mechanisms required by the Controller's local law (such as Standard Contractual Clauses) upon written request.

9. Data Retention and Deletion

The Processor retains Personal Data only for as long as necessary to provide the Saberra service under the following schedule:

- Source Email records: retained in the Controller's Notion workspace for audit purposes; Controller may delete at any time;
- Candidate Records: retained until reviewed (approved or rejected); rejected records are archived (not deleted) to preserve audit trail -- the Controller may delete archived records at any time;
- Approved Canon records: retained until the Controller deletes them from their Notion workspace;
- Processing Events audit log: retained for twelve (12) months by default; earlier deletion available upon request; and
- On termination: the Processor will revoke all access to the Controller's systems within five (5) business days. All data remains in the Controller's Notion workspace, which the Controller retains under their own Notion subscription. No Personal Data is retained by the Processor following access revocation.

10. Personal Data Breaches

In the event of a Personal Data breach affecting data processed under this DPA, the Processor will:

- Notify the Controller without undue delay and in no event later than seventy-two (72) hours of becoming aware of the breach;
- Provide, to the extent then-known: the nature of the breach, categories and approximate number of data subjects and records affected, likely consequences, and measures taken or proposed to address the breach and mitigate its effects; and
- Cooperate with the Controller in preparing any required notification to relevant regulatory authorities or affected data subjects under Applicable Law.

The Controller is responsible for determining whether notification to any regulatory authority or to affected data subjects is required under Applicable Law and for making any such notifications.

11. Audit Rights

The Controller may, upon thirty (30) days' prior written notice and no more than once per calendar year, request an audit of the Processor's data processing activities under this DPA. The Processor will provide reasonable cooperation and access to relevant documentation, subject to confidentiality obligations owed to other clients. The costs of any audit are borne by the Controller unless the audit reveals a material breach of this DPA by the Processor, in which case costs shall be borne by the Processor.

12. Liability and Indemnification

Each party shall be liable for any damage or harm arising from a breach of this DPA caused by its own acts or omissions. The Processor's aggregate liability under this DPA shall not exceed the fees paid by the Controller in the twelve (12) months preceding the event giving rise to the claim, except in cases of fraud, willful misconduct, or gross negligence.

The Controller shall indemnify the Processor against any claims, fines, or penalties arising from the Controller's failure to comply with its obligations under this DPA or Applicable Law.

13. Governing Law and Dispute Resolution

This DPA is governed by the laws of the State of Delaware, without regard to its conflict of law provisions. The parties expressly agree that the United Nations Convention on Contracts for the International Sale of Goods does not apply to this DPA.

Any dispute arising out of or relating to this DPA shall first be addressed through good-faith written negotiation between senior representatives of the parties. If unresolved within thirty (30) days of written notice, the parties agree to submit the dispute to binding arbitration administered by JAMS under its Streamlined Arbitration Rules and Procedures, with proceedings conducted in English in Wilmington, Delaware. Nothing in this Section prevents either party from seeking injunctive or other equitable relief in any court of competent jurisdiction to prevent irreparable harm.

14. Amendments

This DPA may be amended only by a written instrument signed by both parties, except that the Processor may propose amendments to reflect changes in Applicable Law, Sub-processor terms, or platform architecture by providing the Controller with thirty (30) days' written notice. The Controller's continued use of the service after such notice period constitutes acceptance of the amendment.

15. Severability and Entire Agreement

If any provision of this DPA is held invalid or unenforceable, the remaining provisions shall remain in full force and effect. This DPA, together with the Services Agreement, constitutes the entire agreement between the parties with respect to the subject matter hereof and supersedes all prior agreements, representations, and understandings relating to data processing.

Execution

Each party represents that the signatory below is duly authorized to execute this DPA on behalf of the respective party.

DATA CONTROLLER	SABERRA (DATA PROCESSOR)
Authorized Signature	*Saberra, a Delaware Public Benefit Corporation*
Printed Name and Title	Authorized Signature
Date	Printed Name and Title
	Date

Saberra Data Processing Agreement -- Version 1.0 -- DRAFT FOR REVIEW

Saberra, a Delaware Public Benefit Corporation | Governed by Delaware Law

Companion document: Saberra Platform Technical & Governance Documentation

This document requires review by qualified legal counsel before execution as a binding agreement.