Excavaite Inc.

AI & Data Transparency Statement

Effective Date: May 1, 2026

Our Commitment to Transparency

Excavaite's platform is built for organisations that handle sensitive intellectual property. We believe you have the right to know exactly how your documents are processed, which AI services touch your data, and what protections are in place. This statement explains all of that in plain language.

1. What Excavaite Does With Your Documents

Excavaite Sentry-Creator ingests documents from your authorised sources — SharePoint, Google Drive, Confluence, Git repositories, and email — and applies AI analysis to surface intellectual property signals, prior art, and strategic insights. Here is exactly what happens at each step of the processing pipeline:

Step	What Happens	Data Exits Boundary?	Details
1. Document received	Document arrives via connector or email ingest	No	Received from your authorised source only. No external transmission at this step.
2. Stored in database	Raw document stored in your database	No	Excavaite Private: stored entirely within your infrastructure. Excavaite Cloud: stored in Excavaite's secure cloud.
3. Embedding (vectorisation)	Document content sent to embedding service; vectors returned and stored	Yes — once per document	Sent to an AI embedding provider for vector generation. Provider does not retain document content after processing.
4. AI analysis	Document chunks sent to AI model for IP analysis	Yes — per analysis run	Sent to AI inference provider. Provider does not retain content beyond processing each request.
5. Results stored	Analysis findings, vectors, and metadata stored in your database	No	All results remain in-boundary (Excavaite Private) or in Excavaite's secure cloud (Excavaite Cloud).
6. Web search (optional)	Search query terms sent to web search	Yes — query terms only	Only search query text is transmitted — not document content. This feature can be disabled.

	provider during agent analysis		

2. Which AI Services Are Used

Excavaite uses the following categories of external AI service providers. All providers are sub-processors under Excavaite's data processing agreements and are subject to the same data protection obligations as Excavaite.

Service Type	Providers (current)	What Is Sent	Content Retained?
Document embedding	AI embedding service provider	Raw document content — once per document at ingest only	No — contractually prohibited
AI model inference	AI inference provider	Document content chunks during analysis runs	No — contractually prohibited
Language model (LLM)	May include OpenAI, Anthropic, Google Gemini, and others	Document content chunks for IP analysis and content generation	No — contractually prohibited
Web search	May include Google, Bing, Apple, and others	Search query terms only — no document content	No — query terms only

AI language model providers may include OpenAI, Anthropic, Google Gemini, and others. Web search providers may include Google, Bing, and Apple, and others. Providers may be added or changed without prior notice. The current and complete sub-processor list is always published at excavaite.com/legal/sub-processors.

3. What We Guarantee About Your Data

3.1 Your IP Is Your IP

IP Ownership Guarantee

All documents you ingest, and all analysis outputs derived from those documents, remain your exclusive property. Excavaite acquires no ownership interest in your documents, your IP, or any outputs generated by the platform. This is a contractual commitment — not just a policy statement.

3.2 No Training on Your Documents

No AI Training on Your Content

Excavaite does not use your documents, vectors, or analysis outputs to train, fine-tune, evaluate, or benchmark any AI model — including our own systems. This prohibition is contractually required of all AI service sub-processors. No exceptions.

3.3 Document Content Does Not Appear in Logs

Excavaite's operational logs, error reports, and monitoring systems contain only operational metadata — document IDs, timestamps, service call counts, and performance metrics. Document text, extracted IP content, and analysis findings never appear in logs or telemetry.

3.4 All Transmissions Are Encrypted

Every outbound call to an AI service provider uses TLS 1.2 or higher. Your documents are never transmitted over unencrypted connections. Excavaite provisions and manages the API credentials used for all AI services — you do not need to create accounts with any AI provider.

4. Excavaite Private: Your Data Stays in Your Environment

For customers using Excavaite Private, your data protection is reinforced by architecture:

- All document storage, vector indexes, analysis results, and audit logs remain inside your own infrastructure at all times
- Excavaite has no access to your environment by default — troubleshooting uses diagnostic exports that you control
- The only data that exits your environment is the AI service calls described in Section 1 above
- Your network controls govern outbound access — Excavaite Private operates with a deny-by-default egress policy; only approved AI service endpoints are permitted
- Web search is restricted to an allowlisted set of domains — not open internet access

A detailed architecture diagram of the Excavaite Private trust boundary is provided in the Excavaite Private Deployment Overview document.

5. What the AI Analysis Can and Cannot Do

Important Limitation

AI-based analysis is powerful but not perfect. Analysis outputs are probabilistic and may contain inaccuracies or omissions. Documents exceeding AI model input limits may have portions that are not fully analysed. Excavaite's outputs are tools to support your IP team's work — they are not a substitute for professional legal or patent advice.

5.1 What the Platform Does

- Surfaces potential IP conflicts, similarities, and prior art based on semantic analysis of your documents
- Generates summaries, claim analyses, and strategic insights to assist your IP and legal teams
- Monitors your document repositories continuously for new IP signals
- Provides structured workflows for your team to review, assess, and act on findings

5.2 What the Platform Does Not Do

- Provide legal advice, patent advice, or professional IP counsel
- Guarantee completeness — analysis coverage depends on model input limits and document structure
- Create attorney-client privilege over analysis outputs
- Replace your IP counsel's independent assessment of findings

5.3 Prior Art and Disclosure Obligations

Excavaite's web search and analysis features may surface prior art or publicly available information. If your team encounters prior art through the platform, you may have disclosure obligations under applicable patent rules (for example, the USPTO duty of candour). Your IP counsel — not Excavaite — is responsible for assessing those obligations. Ensure your legal team is involved in reviewing analysis outputs before taking action.

6. Excavaite Cloud Trial: Same Protections Apply

When you access Excavaite through an Excavaite Cloud trial — typically sending 10 to 20 representative documents to evaluate the platform — the same data protections described in this statement apply from day one. Trial data is not treated differently from production data. If you subsequently transition to Excavaite Private, all Excavaite Cloud trial data is deleted from Excavaite's infrastructure within 30 days of your confirmed Excavaite Private deployment.

7. Your Rights and Controls

- Connector scope: you define exactly which document sources Excavaite can access. Access is not granted organisation-wide by default.
- Web search on/off: the agent web search feature can be disabled entirely.
- Audit log export: complete audit logs of all document ingest events, user actions, and AI service calls are available for export at any time.
- Data deletion: on contract termination, you can request deletion of all Customer Content and Derived Outputs. Excavaite will confirm deletion in writing within 60 days.
- Sub-processor objection: you may object to new sub-processors. If Excavaite cannot accommodate the objection, you may terminate your agreement without penalty.

8. Questions and Transparency Requests

We welcome questions about how our AI systems work and how your data is used. If you have a question not answered in this statement, or would like to request a technical review session with the Excavaite team:

Contact: support@excavaite.com

Excavaite Inc., [Street Address], [City], [State] [Zip Code]

Excavaite Inc. © 2026 — excavaite.com/legal