DarkMatter

LEGAL AND COMPLIANCE OVERVIEW

Execution Lineage and Audit Trail for AI Agent Pipelines

darkmatterhub.ai | hello@darkmatterhub.ai | Version 1.0

What DarkMatter Does

DarkMatter is an independent, external execution history layer for AI agent pipelines. Every agent action is recorded as an immutable context commit with SHA-256 cryptographic hash chaining. The resulting audit trail is tamper-evident, externally hosted, and exportable as a portable proof artifact.

Regulatory Alignment

DarkMatter is designed to support compliance with the following frameworks. Customers should consult their legal counsel to confirm applicability to their specific deployment.

Framework	Relevant Requirement	How DarkMatter Helps
EU AI Act Art. 12 and 19	Automatically generated, tamper-evident logs retained for at least 6 months for high-risk systems	Immutable commit chain with timestamps, retention policies, and exportable audit artifacts
US State AI Laws (CO, CA, others)	Explainability and audit trail requirements for consequential automated decisions	Full replay of decision chain shows exactly what each agent decided and in what order
Financial Sector (SEC, FCA, MAS)	AI-assisted decision documentation and explainability for regulated activities	Cryptographic chain proves decisions were not modified after the fact
Healthcare AI	Clinical AI decision documentation for liability and regulatory purposes	Per-step attribution with agent identity, model used, and timestamped outputs

Data Handling and Privacy

Data in transit: All API traffic encrypted with TLS 1.3.

Data at rest: Encrypted at rest via Supabase AES-256 managed encryption.

BYOK encryption: Enterprise: client-provided AES-256-GCM key. DarkMatter stores only ciphertext. Client key never stored.

Data residency: Default: hosted by DarkMatter (US). Enterprise: self-hosted deployment inside client network available.

Retention: Free: 30 days. Pro: 1 year. Enterprise: configurable per agent. Data deleted after 30-day grace period on account closure.

Sub-processors: Supabase (database), Railway (hosting), Resend (transactional email), Cloudflare (DNS and CDN).

Data subject requests: Customers can export or delete all context data via the dashboard or API at any time.

Independence Guarantee (Hosted Enterprise Plan)

On the hosted Enterprise plan, the audit trail is stored on DarkMatter servers external to the customer's infrastructure. Because the customer cannot modify records on DarkMatter's systems, the audit trail carries the same independence as a third-party auditor's records. BYOK encryption ensures DarkMatter cannot read payload content, addressing both independence and confidentiality requirements simultaneously.