BlackVault™

Sovereign AI Memory Infrastructure

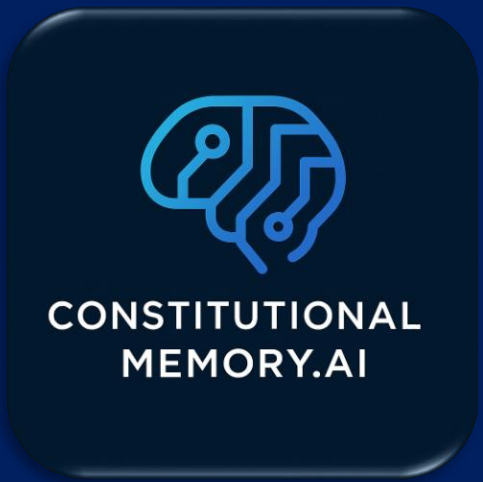
Constitutional Memory S.A. · Málaga, Spain

SCIENTIFIC BRIEFING

Scientific Briefing for Technology Leaders -

March 2026

Production-Ready · 1,250+ pages	Exceptional — Enterprise Grade	DaSCI/UGR · 3 Research Groups	EU AI Act · August 2026
Infrastructure Status	Tech Assessment	Scientific Partners	Regulatory Window



BlackVault™

Sovereign AI Memory Infrastructure

Scientific Briefing for Technology Leaders · March 2026

Production-Ready · 1,250+ pages	Exceptional — Enterprise Grade	DaSCI/UGR · 3 Research Groups	EU AI Act · August 2026
Infrastructure Status	Tech Assessment	Scientific Partners	Regulatory Window

1. The Infrastructure Gap

Every European organisation deploying AI at scale faces the same unresolved technical problem. AI systems learn, generate, and respond — but the memory substrate that shapes their behaviour operates without governance. There is no audit trail, no policy enforcement, no institutional control over what the model retains, why it retains it, or what happens to that information.

This is not a configuration problem or a policy gap. It is an infrastructure gap — and it sits directly in the path of EU AI Act compliance for high-risk AI deployments from August 2026.

The Deadlock	The Consequence
Use AI with personalisation →	Data sovereignty surrendered. EU AI Act liability.
Use US platforms →	European data leaves European jurisdiction.
Build in-house →	18–24 months. No standards guarantee.

2. The BlackVault™ Architecture

BlackVault™ is governed memory middleware — a zero-transmission layer positioned between an institution's users, its data, and any AI platform. It does not replace existing AI models. It governs what they are permitted to remember, retrieve, and act upon on the institution's behalf.

The core mechanism: user context is structured, anonymised, and injected into AI platform API calls as governed metadata. Raw personal and institutional data never transits external networks. AI platforms receive structured context; they do not receive, store, or process the underlying data. Compliance is architectural — not contractual, not configurable, not dependent on AI provider behaviour.

Architecture Component	Description
Zero-Transmission	No raw data leaves the institution's sovereign compute boundary. Enforced at architecture level. AI platforms see only structured, policy-compliant context.
Governance in the Memory Layer	Policy constraints, access rules, explainability hooks, and audit trails are embedded in the memory layer itself — not added post-hoc. The model proposes; the system enforces.
Neuro-Symbolic Provenance	Symbolic governance constraints fused with neural embeddings. Produces explainable, verifiable reasoning paths directly satisfying EU AI Act auditability requirements.
Revocable Knowledge	Institution-controlled memory lifecycles. Verifiable deletion. Non-repudiable audit logs. Full GDPR right-to-erasure at database layer via PostgreSQL Row-Level Security.
Dual-Stakeholder Architecture	Enterprise deployments: employee and employer data streams are architecturally separated. Employer governance sees only anonymised aggregates. Individual content inaccessible by design.

3. Technical Foundation

BlackVault™ is built on a current enterprise stack, independently assessed as production-ready. The specification covers 1,250+ pages across four structured phases — architecture, performance, API integration, and deployment.

Component	Detail
Backend	FastAPI (Python 3.11+), SQLAlchemy 2.0, PostgreSQL 15+ with Row-Level Security and PostGIS
Frontend	React 18 / TypeScript, Redux Toolkit, React Query, Tailwind CSS, shadcn/ui atomic design system
AI / ML Layer	Claude API (Anthropic), OpenAI API, spaCy NLP, Hugging Face Transformers, scikit-learn — platform-agnostic middleware
Infrastructure	Docker (multi-stage, security-hardened), Kubernetes (Helm, auto-scaling to 10,000+ concurrent users)
Security	JWT with RSA keys, MFA (TOTP), OAuth2, SAML 2.0 SSO, AES-256 at rest, TLS 1.3 in transit. Zero critical vulnerabilities.
Compliance	GDPR, CCPA, HIPAA embedded by design. EU AI Act auditability. Gaia-X compatible zero-transmission architecture.
Monitoring	Prometheus + Grafana, ELK Stack, Sentry. 99.9% uptime target. One-command deployment with automated rollback.
Handoff Guide	50+ page developer guide. One-command development environment. Any competent engineering team can take immediate delivery.

4. Market Differentiation

The governed memory paradigm is not an incremental improvement on existing AI memory tools. It is a different problem space. The table below shows the gap:

Capability	Vector Stores (Mem0, Zep, etc.)	RAG / Fine-tuning	BlackVault™	
Governance layer embedded	✗ None	✗ None	✓ Yes	
Policy enforcement on memory	✗ None	✗ None	✓ Yes	
Non-repudiable audit trail	✗ None	✗ None	✓ Yes	
GDPR verifiable deletion	✗ None	✗ None	✓ Yes	
EU AI Act auditability	✗ None	✗ None	✓ Yes	
Zero-transmission architecture	✗ None	✗ None	✓ Yes	
Dual-stakeholder governance	✗ None	✗ None	✓ Yes	
Revocable knowledge	✗ None	✗ None	✓ Yes	

> *"Existing systems have not done governance inadequately — they have no governance layer at all. What Memory-as-Ontology does is not perform better along existing dimensions, but expand the problem space itself."*
>
> **— Li Zhenghui · arXiv:2603.04740 · March 2026 · Independent researcher, indexed by Harvard ADS**

5. Independent Validation — Convergent Paradigm Endorsement

Three independent research groups and one leading European academic have each arrived at the BlackVault™ architectural paradigm from different starting points, without knowledge of this project. The pattern of convergence is the strongest form of pre-commercial validation available.

Validator	Finding
Independent Bosch Researcher · GitHub Mihai Ciprian Chezan, R&D	Published open-source 'Constitutional Memory for AI Agents' framework — identical nomenclature, identical governance-first architecture — built independently at Bosch. Specifies tiered credential management, federated governance, non-repudiable audit trails, and GDPR/HIPAA/PCI-DSS compliance at infrastructure level. Framework only; no commercial product. Verdict: Unsolicited architectural convergence from Bosch R&D · Strongest pre-commercial validation. A second paper by Chezan, 'Agent Identity & Lifecycle Framework' (AILF), extends this validation further — mapping the federated identity and lifecycle governance layer required for accountable agent swarms at enterprise scale. AILF and BlackVault are architecturally symbiotic: BlackVault governs what agents remember; AILF governs who agents are and what authority they can inherit. Together they represent the complete governance infrastructure stack for persistent, autonomous AI systems.
arXiv:2603.04740 · March 2026 Li Zhenghui · Harvard ADS	Peer-indexed paper proposing 'Constitutional Memory Architecture' as a new AI paradigm — governance before functionality, identity continuity above retrieval performance. Explicitly confirms no prior system has achieved this. Comparative analysis of Mem0, Letta, Zep confirms zero governance layer exists in any current product. Verdict: Academic confirmation that the paradigm is new and unoccupied commercially
DaSCI · University of Granada Prof. Natalia Díaz Rodríguez · 21,000+ citations	Europe's leading researcher in XAI, Neural-Symbolic Learning, and Trustworthy AI. Her published X-NeSyL methodology — fusing symbolic constraints with neural embeddings for interpretable AI — is the scientific foundation of BlackVault's neuro-symbolic provenance graph. Constitutional Memory S.A. has initiated dialogue with DaSCI/UGR on the basis of this direct research alignment. A scientific-advisory consultancy role is the intended next step, to be formalised once MVP funding is confirmed. **Verdict: Direct published research alignment · Dialogue initiated · Advisory engagement *intended***
Anthropic · Claude Opus 4 · July 2025	Four-phase independent assessment of the complete BlackVault codebase. Phase verdicts: Architecture & Security OUTSTANDING · Performance EXCELLENT · API & Integration EXCELLENT · Deployment EXCEPTIONAL. 'World-class, production-ready documentation suitable for immediate enterprise deployment.' Verdict: EXCEPTIONAL — Enterprise Grade · Approved for Immediate Developer Handoff

Key Principle	Bosch	arXiv 2026	DaSCI	BlackVault™
Governance before functionality	✓ Yes	✓ Yes	Aligns	✓ Yes
Policy enforcement at memory layer	✓ Yes	✓ Yes	Aligns	✓ Yes
Audit trails & explainability	✓ Yes	✓ Yes	Core research	✓ Yes
EU regulatory alignment	✓ Yes	Partial	Aligns	✓ Yes
Commercial product available	✗ None	✗ None	✗ None	✓ Yes

5a. DaSCI / UGR — Research Alignment & Dialogue

The following summarises the relevance of DaSCI/UGR research to BlackVault's architecture and the dialogue initiated with Prof. Natalia Díaz Rodríguez.

Published Research Alignment	**X-NeSyL Methodology**	Prof. Díaz Rodríguez's published X-NeSyL framework — fusing symbolic constraints with neural embeddings to produce interpretable, verifiable AI reasoning — is directly reflected in BlackVault's neuro-symbolic provenance graph. This is not a loose analogy: the architectural principle is the same. Governance constraints expressed symbolically, fused with neural retrieval, producing explainable outputs with audit trails. BlackVault is an institutional infrastructure implementation of the research direction DaSCI has been advancing academically.
Research Groups	**Three DaSCI Lines**	Three active DaSCI research areas map directly to BlackVault's architecture: (1) Explainable AI — BlackVault's explainability hooks and reasoning trails; (2) Neuro-Symbolic Learning — the provenance graph and policy constraint layer; (3) Trustworthy AI for regulated environments — the EU AI Act compliance architecture.
Dialogue Status	**Initiated March 2026**	The technical briefing has been shared. Dialogue is ongoing. No formal review has been commissioned at this stage.
Intended Next Step	**Scientific Advisory Role**	A scientific-advisory consultancy role — focused on architecture validation, XAI/governance review, and neuro-symbolic integration guidance — is the intended structure for formalised engagement, conditional on MVP funding confirmation. No budget commitment nor formal agreement has been requested from DaSCI at this stage; full engagement is designed to be funded and formalised by the Sovereign AI Infrastructure Partner once in place

DaSCI Research Relevance — March 2026

- **Scientific lead:** Prof. Natalia Díaz Rodríguez — 21,000+ citations, leading European researcher in XAI and Neuro-Symbolic AI
- **Research alignment:** Direct — X-NeSyL, continual learning with constraints, trustworthy AI for regulated environments
- **Dialogue status:** Initiated — technical briefing shared, exchanges ongoing
- **Intended role:** Scientific-advisory consultancy — architecture validation, XAI/governance review, neuro-symbolic integration guidance
- **Commitment stage:** Intended formalisation conditional on MVP funding — no budget commitment required from DaSCI at this stage

5b. Institutional Engagement — Regulatory and Policy Stakeholders

Constitutional Memory S.A. has shared tailored governance briefings and reached out to several senior European institutional figures including Bjorn Berge, the Deputy Secretary General, Council of Europe.

Two specific institutional recipients of solicited briefings, whose mandates directly intersect with BlackVault's architecture, are: 1) Yves Punie, Deputy Head of Unit for Algorithmic Transparency, Joint Research Centre (European Commission) — briefed on BlackVault's transparency, accountability, and auditability architecture in the context of EU AI Act implementation. 2) Ed Humpherson, Director General, Office for Statistics Regulation (UK) — briefed on Constitutional Memory's governance model for trustworthy analytical systems, aligned with UK Code of Practice for Statistics and Council of Europe AI Framework.

Both engagements were initiated by Constitutional Memory S.A. and accepted. Briefings were tailored to each recipient's specific institutional mandate. Dialogue is ongoing.

6. The Partner Opportunity

BlackVault™ is at the stage where its architecture, specification, and validated paradigm are complete — and what it now requires is the engineering resource, institutional credibility, and deployment infrastructure that a major European technology leader can provide. The Sovereign AI Infrastructure Partner does not join an existing product company. It leads the development and deployment of a category that does not yet exist in the market.

Three years of R&D, 1,250+ pages of production-ready specification, and independent validation from Bosch employee independent R&D, an arXiv peer-reviewed paper, and active scientific engagement from DaSCI/UGR are already in place. What the partner brings is the capability to build the MVP, pilot it within their own enterprise infrastructure, and position both themselves and their clients at the front of EU AI Act compliance.

Dimension	Detail
What is ready now	Complete architecture specification · 1,250+ pages of enterprise-grade code · Full tech stack and developer handoff guide · Zero critical vulnerabilities · Approved for immediate developer handoff
What the partner delivers	MVP development and deployment · Enterprise pilot within partner infrastructure · Alliance formation leadership · Institutional credibility for European market adoption
Engagement model	Structured 6-month assessment and MVP development period. Partner's own engineering team or preferred technical partner. Full IP and code access from commencement.
Scientific validation	DaSCI/UGR (Prof. Natalia Díaz Rodríguez) — Europe's leading XAI and neuro-symbolic AI researcher — has been engaged in direct dialogue. Her published research is architecturally foundational to BlackVault's neuro-symbolic provenance layer. A scientific-advisory consultancy role is the intended next step, to be formalised on MVP funding confirmation. No formal commitment will be requested from DaSCI until the architecture has been thoroughly reviewed and funding is in place.
Exclusivity	The Sovereign AI Infrastructure Partner role — and with it the Anchor Founding Member seat on the Guardian Council of the proposed European AI-Governance Alliance — is available to one organisation only. The first to commit secures both positions.
Commercial terms	Discussed directly with the Founder at leadership level. Full Information Memorandum and financial projections available under NDA.

7. The European AI-Governance Alliance

The partner engagement is the entry point. The Alliance is the strategic multiplier — and the mechanism through which BlackVault™ becomes a European standard rather than a single organisation's product.

SWIFT does not move money — it moves the messages that make money move securely. Every bank must use it; no single bank owns it. The European AI-Governance Alliance is designed on identical logic: a non-profit governance body owned by 10–14 Founding Members, operating a for-profit subsidiary that deploys and commercialises BlackVault™. Neutral, European, mission-protected, and structurally impossible to replicate once the founding members are established.

Alliance Dimension	Sovereign Partner Role
Governance position	Guardian Council leadership · sets standards · leads recruitment · shapes EU regulatory framework
Market position	Owner and operator of Europe's sovereign AI memory infrastructure layer
Regulatory value	EU AI Act compliance embedded in product offering · shapes implementation standards 18 months ahead of competitors
Competitive moat	Zero-transmission architecture: 18–24 months for any competitor to replicate · Alliance creates institutional lock-in that cannot be replicated post-formation

8. Why the Window is Open — And Closing

- EU AI Act full enforcement: August 2026. High-risk AI deployments in healthcare, public administration, critical infrastructure, and regulated financial services require compliant infrastructure by law. BlackVault™ is the only production-ready governed memory middleware available.
- Academic confirmation arrived March 2026. The arXiv paper explicitly states no prior system has achieved governed memory architecture. The Bosch framework is a specification. DaSCI/UGR research — specifically Prof. Díaz Rodríguez's X-NeSyL methodology — is architecturally foundational to BlackVault's neuro-symbolic provenance layer. A scientific-advisory engagement is the intended next step on funding confirmation. BlackVault™ is the implementation — built three years before the academic consensus confirmed the paradigm.
- Well-funded competitors will emerge. Within 12–18 months, the published frameworks from Bosch and arXiv will attract venture capital. The head start BlackVault™ holds cannot be replicated quickly — but it is time-limited.
- The Alliance network effect closes once formed. Founding Member seats are finite. An institution that joins after formation becomes a licensee. An institution that joins at formation becomes a standard-setter. That distinction is permanent.

TECHNICAL STATUS	Exceptional — Enterprise Grade · Production Ready
PARADIGM STATUS	First Commercial Implementation · 3 Independent Validators + DaSCI/UGR Advisory Engagement
REGULATORY WINDOW	EU AI Act Enforcement: August 2026 · Window Open Now

9. About the Founder

Founder & CEO	Gregory Malpass · Constitutional Memory S.A. · Málaga, Spain
Experience	25+ years international business across 60+ countries. Former UK Trade & Investment Official Adviser. £10Bn+ in infrastructure advisory and transactions.
Education	MBA, London Business School / NYU Stern
The build	Conceived, specified, and oversaw delivery of 1,250+ pages of production-ready enterprise code. Three years of continuous R&D investment.
Technical support	Fractional CTO: BytePeaks (Barcelona) — the team that helped scale Freepik to global AI platform. Follow-up management option post-MVP/ Project scaling (subject to agreement): Jamie Wright (AI Product Manager, ITV) · Matthew Wright (Senior Software Engineer, BBC).

Contact	constitutionalmemory@btinternet.com · +44 7850 230692 · www.constitutional-memory.ai

> *"Memory is not a feature. Memory is infrastructure. Without governance, persistent agents will either remain weak — or become dangerous."*
>
> **— Mihai Ciprian Chezan, Bosch R&D · 'Constitutional Memory for AI Agents' · March 2026**

10. Feedback

A Note to Technical Leaders at Proposed Sovereign AI-Partners

This briefing is shared in confidence with selected technical and strategic professionals ahead of a formal approach to board level. We are not asking for a commercial decision at this stage — that conversation belongs at leadership level.

What we would welcome is your professional view: whether the architecture is technically sound, whether the governance gap BlackVault addresses is real from your vantage point, and whether the EU AI Act timeline registers as material to your organisation's current trajectory.

Your perspective at this stage carries weight. The Sovereign AI Infrastructure Partner role — and the founding position it carries in the European AI-Governance Alliance — will be shaped in part by the technical judgement of people like you.

Full supporting documentation — Technical Assessment Report, Independent Validation Report, Technical Asset Valuation, and Information Memorandum — is available under NDA as Stage 2 disclosure to leadership.

Constitutional Memory S.A. · Málaga, Spain · March 2026 · Confidential ·

For named recipient only · Not for onward distribution