



LEGAION™

BY AIDVOCATES, INC. · DELAWARE, USA

Sovereign Legal AI for Enterprise.

Architecture, Compliance, and Operational Framework.

A technical reference for General Counsels, Big Law partners, and M&A; teams evaluating verified-source legal AI under EU sovereignty constraints — built around **seven patent-pending technologies**, dual-model architecture, and contractually enforced zero-retention.

PREPARED FOR

Executive Legal Decision-Makers

General Counsel · Managing Partners · Heads of Compliance
Senior Associates evaluating sovereign legal AI infrastructure.

7 PATENTS PENDING (UPRP) · EU-SOVEREIGN INFRASTRUCTURE · SOC 2 TYPE II (INITIATED 2027) · ZERO-RETENTION ARCHITECTURE

AIDVOCATES, INC. · 136 MADISON AVENUE, NEW YORK, NY 10016 · EU R&D: KATOWICE, POLAND

01 · EXECUTIVE SUMMARY

Why this brief exists.

Generic large language models hallucinate legal citations between **17% and 29%** of the time, depending on the jurisdiction and query class (Stanford HAI, Reuters Legal, 2024). Public-cloud deployment creates documented exposure under EU AI Act Article 28 and GDPR Articles 28 and 44. Public-API providers typically retain prompt and output data for 30 days; some retain longer under stated training-improvement clauses.

CITATION VERIFICATION	INFRASTRUCTURE	RETENTION
P.454531	EU-only	Zero
Three-stage source check · ISAP/EUR-Lex/USPTO	SP10 · Azure EU · AWS Bedrock EU	Contractually enforced · no model training

What enterprise legal teams actually face.

Mata v. Avianca (2023, S.D.N.Y.) established the precedent: attorneys submitting AI-generated briefs containing fabricated case citations face Rule 11 sanctions and reputational damage. Subsequent rulings in Park v. Kim (2024) and in re Steven A. Schwartz disciplinary proceedings reinforced that the burden of citation verification rests on the submitting attorney — regardless of the AI tool's marketing claims.

Concurrently, EU AI Act Article 14 requires meaningful human oversight for high-risk AI systems used in legal practice. Article 50 mandates transparency about AI involvement in legal output. NIS2 directives apply to legal-services firms above defined revenue thresholds, requiring documented incident response and supply-chain risk management for AI vendors processing client data.

Seven engines. One verification protocol.

LEGAION is not a wrapper around a single foundation model. The platform operates on a **dual-model architecture** (generator + verifier) coordinated through patented modules. Each module addresses a discrete failure mode of generic legal AI — fabrication, semantic drift, jurisdictional conflict, or strategic blindness.

P. 454531**Verifier Engine™****P. 454593****Sentinel™**

Semantic change detection in contracts and regulatory documents. Identifies modified clauses, hidden insertions, and material redlines across versions.

P. 454607**Predict™**

Behavioural prediction of judicial outcomes based on jurisdiction-specific case-law corpora and judge-level decision histories.

P. 454612**Counter™**

Adversarial argument generation with structured weakness mapping of opposing counsel positions.

P. 454628**Operator™**

Coordination layer routing prompts across model providers and verification stages with deterministic audit trail.

P. 454641**Witness Prep™**

Vocal stress and consistency analysis for deposition and witness preparation scenarios under controlled session conditions.

P. 454659**Cross-Border Shield™**

Risk mapping and remediation across 32+ jurisdictions with conflict-of-laws detection at the clause level.

Where your data actually lives.

Sovereignty in legal AI is not a marketing claim — it is a verifiable chain of named operators, named regions, and contractual no-egress guarantees. LEGAION publishes its full sub-processor list and infrastructure topology to enable independent verification by client compliance teams.

COMPUTE TIER 1

OVHcloud

France-headquartered · EU-only data plane

COMPUTE TIER 2

Azure EU

Frankfurt · Madrid · Paris · Anthropic Claude EU

COMPUTE TIER 3

AWS Bedrock EU

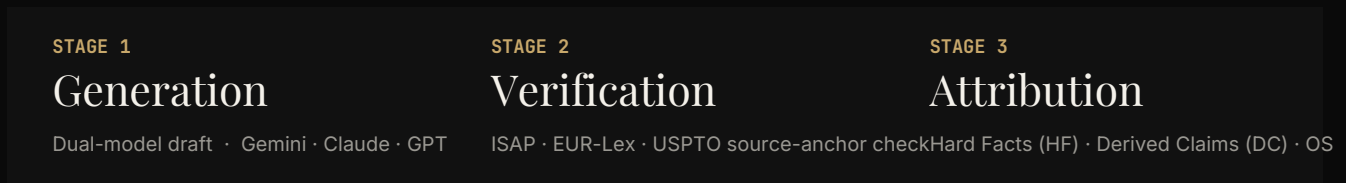
Frankfurt · DPA-enforced no training

What this rules out.

Compliance posture.

How verified output actually gets produced.

Every output passes through the same deterministic pipeline regardless of which generation model produced the draft. The Verifier Engine treats the generator's output as untrusted input and re-validates every factual claim, citation, and statutory reference against authoritative primary sources.



Output classification.

Hard Facts (HF) — verified against official publications, marked with source URI and verification timestamp. **Derived Claims (DC)** — conclusions with documented evidentiary chain back to Hard Facts. **Opinion Statements (OS)** — clearly labelled, never presented as fact. This three-tier attribution is enforced at the rendering layer and cannot be bypassed by prompt engineering.

Audit trail.

Every session produces a tamper-evident audit log capturing model selection, verification outcomes, source URIs, and final attribution per output segment. Logs are encrypted at rest, scoped per-organisation, and purged on the schedule defined in the customer's data retention agreement (default: zero retention beyond session end). Super-admin role can export per-organisation audit packages for regulatory inquiry.

Limits and disclaimers.

LEGAION delivers verified facts and auditable conclusions. Outputs depend on input quality and the freshness and availability of verified legal sources. Professional legal judgment and client representation remain the exclusive domain of licensed attorneys. LEGAION augments — it does not replace — qualified legal counsel.

Next steps.

LEGAION engagements begin with a 30-minute scoping call under NDA, followed by a sandboxed pilot in your environment. No client data leaves your control during evaluation. Pricing is published per Enterprise tier; volume and multi-jurisdiction discounts available for managed legal departments and Big Law firms.

STEP 1

Scoping Call

30 min · NDA on request · no commitment

STEP 2

Pilot

2-week sandbox · customer-controlled environment

STEP 3

Deployment

Enterprise SLA · EU-only data plane · SSO

Direct contacts.

Commercial inquiries — office@aidvocates.com · Data protection — dpo@legaion.com · Security disclosure — security@legaion.com

Document control.

Document version: v.2026.05. Supersedes all prior technical briefs. This document is confidential and prepared exclusively for the named recipient. Reproduction or onward distribution requires written consent from Aidvocates, Inc. For the most recent revision and full Service Level Agreement, contact your assigned LEGAION account lead or visit www.legaion.com.

Signature.

Aidvocates, Inc. · 136 Madison Avenue, New York, NY 10016, USA · Delaware File No. 10564433 · EU Engineering: Aidvocates Group sp. z o.o. · ul. Hutnicza 6, 40-241 Katowice, Poland.