

NiaShield

EU AI Act – Regulation (EU) 2024/1689 – what the architecture answers for you.

For organisations deploying AI under the EU regime. The obligations of the AI Act answered at two layers — NiaShield, the application a regulated person uses, and Gateway Sessions, the enforcement plane in front of the models. Highlighted rows are the obligations live on 2 August 2026. Every claim traces to the cited article.

ARTICLE §	WHAT IT REQUIRES	HOW THE ARCHITECTURE ANSWERS IT	LAYER	STATUS
Art. 50	Transparency: people are told when they are interacting with an AI system.	Disclosure to affected persons is the deployer's act . The architecture supplies the controlled, recorded environment that makes the disclosure defensible — it does not perform the notice itself. <i>Deployer transparency stays on the 2 Aug 2026 schedule; the Digital Omnibus moves only provider-side Art. 50(2) watermarking to 2 Dec 2026.</i>	NIA · GTW	✓
Art. 10	Data governance: relevant, representative data; minimisation; security safeguards.	NiaShield processes content without retaining it at rest; session records die by key destruction; keys are customer-resident — governed data never leaves the deployer's control. Gateway locks egress to American systems and retains no content.	NIA · GTW	✓
Art. 12	Record-keeping: automatic logging of events over the system lifetime; traceability.	Every session emits a Certificate of Incineration™ — an Ed25519-signed, independently verifiable record that the event occurred and the data was destroyed. The deployer holds it and presents it. Operational logs stay in the deployer's tenant, content-free; the deadline ledger is write-once.	NIA · GTW	✓
Art. 13	Transparency to deployers: operation interpretable; instructions for use.	The no-retention behaviour is documented and stated, not implied. Gateway ships as a declarative template the deployer reviews in full before use — what it does and where its boundaries sit are inspectable.	NIA · GTW	✓
Art. 14	Human oversight: ability to monitor, intervene, and halt the system.	Gateway's born-once, non-extendable deadline is oversight expressed in architecture — a session cannot outlive its mandate, and the custodian's stop-and-destroy is the structural equivalent of the Article's interrupt-and-halt. NiaShield flags high-signal PII before forwarding, giving a human a decision point. The oversight policy is the deployer's to set.	NIA · GTW	✓
Art. 15	Accuracy, robustness, cybersecurity over the lifecycle.	Separation of duties across four managed identities, RBAC-only data stores, default-deny network, customer-resident keys, and <code>verify_sovereign_isolation</code> — which the deployer re-runs in their own tenant — give demonstrable, re-provable security controls.	NIA · GTW	✓
Art. 26	Deployer obligations: assign oversight; monitor operation; report incidents.	The architecture supplies the recorded, controlled substrate and the monitoring signal. Monitoring and reporting under Art. 26(5) remain the deployer's act — the product gives the evidence to act on, not the act itself.	NIA · GTW	✓
Art. 5	Prohibited practices (manipulation, exploitation, prohibited categories).	Out of scope by design: the architecture neither performs nor enables a prohibited practice — including the Digital Omnibus's new Art. 5 bans on AI that generates NCII or CSAM. Whether a given use is prohibited is the deployer's determination; the substrate adds no prohibited capability.	NIA · GTW	✓

And here's what the deployer still owns.

The AI Act's substantive obligations attach to roles — chiefly the deployer. The architecture supports each with evidence and tooling, but the action is the deployer's. This is the honest half of the crosswalk.

Why this page matters. No product makes an organisation AI-Act compliant — compliance is governance the deployer performs. Hand this page to the compliance lead and the CISO: it shows exactly where NiaShield and Gateway evidence plugs into the deployer's obligations. The legal classification of a given system, and the conclusions that follow, are the deployer's to make with qualified counsel — the architecture supplies the product facts and the evidence.

ARTICLE §	WHAT THE DEPLOYER IS ON THE HOOK FOR	WHAT THE ARCHITECTURE GIVES TO MAKE IT EASIER
Art. 26(1)	Use the high-risk system per the provider's instructions for use.	Instructions and the documented no-retention behaviour ship with the deployment; the deployer operates within them.
Art. 26(2)	Assign human oversight to competent, trained, resourced persons.	The stop-and-destroy boundary and the PII decision point give those persons a defined place to act. Competence and assignment are the deployer's.
Art. 26(5)	Monitor operation; inform the provider and market-surveillance authority of risks; suspend on risk.	Operational telemetry and the session record live in the deployer's tenant, ready to pull. The monitoring and the notification are the deployer's act.
Art. 26(6)	Keep the automatically generated logs for the required period.	Logs and Certificates of Incineration™ are customer-held in standard Azure services — retention follows the deployer's policy.
Art. 50	Inform natural persons they are interacting with an AI system, where required.	The controlled, recorded environment makes the disclosure defensible; the deployer issues the notice.
Art. 4	AI literacy: ensure staff operating the system have sufficient understanding.	Architecture documentation and the published design support a literacy programme; the programme itself is the deployer's.
Art. 72	Cooperate with post-market monitoring; surface relevant operational data.	Content-free operational telemetry and verifiable certificates give monitoring data without exposing governed content.
GDPR overlap	Where personal data is processed, GDPR applies concurrently (DPIA, lawful basis).	Zero-persistence and customer-resident keys reduce the personal-data surface; the DPIA and lawful-basis analysis are the deployer's, with counsel.

The bottom line.

The EU AI Act answers to roles and risk tiers, not to vendors. Its heavy obligations attach to the deployer. The honest position — and the strong one — is this: no product makes an organisation compliant. What NiaShield and Gateway Sessions provide is the technical evidence layer that makes a deployer's obligations satisfiable, and the artifacts that let the deployer prove it.

Compliance is the deployer's. The proof is what the architecture supplies.

Why two layers, not one.

The same obligation lands differently depending on where it sits. **NiaShield** answers where the deployer's data duties live — governance, record-keeping, minimisation — with zero-persistence and the **Certificate of Incineration™** as the held, verifiable evidence. **Gateway Sessions** answers where the system-control duties live — bounding the session, oversight-as-architecture, robustness, and isolation the deployer can re-prove on demand. One design language, both halves of the obligation set.

On the 2 August 2026 date.

2 August 2026 is when enforcement begins and the Article 50 deployer transparency obligations apply. The most operationally demanding high-risk obligations are subject to the Digital Omnibus deferral — stand-alone Annex III systems to 2 December 2027, AI embedded in regulated products to 2 August 2028, and provider-side Art. 50(2) watermarking to 2 December 2026 — which take legal effect only on publication in the Official Journal. The controlling dates are those in the published OJ text. The posture here is to build ahead of the regime, not to wait for the deferral.

Steve McKim

CEO & Founder, Heaviside AI

steve@heavisideai.com · niashield.com · heavisideai.com

NiaShield, SDIP-6, Certificate of Incineration™, Gateway — Heaviside AI, LLC. Obligations cited to Regulation (EU) 2024/1689 as published in the Official Journal; article summaries are paraphrased for mapping and the controlling text is the Regulation. This is an architecture-to-obligation mapping, not legal advice; classification of a system and the resulting obligations are the deployer's determination with qualified counsel. U.S. Prov. App. 64/042,610 (Apr 17 2026) · 64/068,643 (May 18 2026) · Inventor of record: Steve McKim.