EU AI Act — Article 26 Deployer Obligations Matrix

Runtime-facing duties and how Pipelock evidence maps

This matrix summarises the runtime-facing duties of Article 26 for deployers of high-risk AI systems and explains what Pipelock evidence supports under each paragraph. Pipelock is an evidence substrate, not a compliance solution. The deployer retains policy ownership, retention period, review cadence, and formal sign-off. Always read the official Official Journal text and consult qualified legal counsel before relying on any single page as a compliance checklist.

Runtime-facing duties of Article 26 (paragraphs 1, 2, 4, 5, 6)

Article 26 paragraph	Obligation (paraphrased from the OJ text)	Pipelock evidence that supports it	What the deployer still owns
26(1)	Take appropriate technical and organisational measures to use the system in accordance with the provider's instructions for use.	Posture-verify CLI with score model and CI gate, configuration validation at startup, deployment guidance, configuration hash recorded in each emitted record.	Operating within the documented deployment profile, training staff on approved configurations, change management for config drift.
26(2)	Assign human oversight to natural persons with the necessary competence, training, authority, and support.	HITL approval flow on the `ask` action with terminal prompts, kill switch from four independent sources (config, API, SIGUSR1, sentinel file), per-action audit trail.	Selecting oversight personnel, training and authorisation policy, escalation runbooks, on-call coverage.
26(4)	Ensure input data is relevant and sufficiently representative of the intended purpose, to the extent the input is under the deployer's control.	Input scanning on MCP tool arguments, fetch-proxy URL parameters, forward-proxy bodies, request-body scanning with class-preserving redaction.	Defining what "relevant and representative" means for the use case, dataset curation, input governance upstream of the proxy.
26(5)	Monitor the system's operation based on the instructions for use and inform the provider and, for serious incidents or identified risks, the market surveillance authority without undue delay.	Prometheus metrics endpoint, `/health` and `/ready` endpoints, hardcoded event severity taxonomy with configurable emission threshold, webhook and syslog sinks to any SIEM, real-time block-reason headers.	Defining the serious-incident threshold, operating the SIEM, drafting incident notifications, regulator and provider communication.
26(6)	Keep the logs automatically generated by the system for at least six months, to the extent those logs are under the deployer's control. Longer retention applies where other Union or national law requires it, in particular data-protection law.	Structured JSON event lines with stable field names, hash-chained flight recorder, optional Ed25519 signed receipts, no vendor-locked binary format, exportable to any retention-controlled store.	**The retention period itself.** Pipelock emits to the sinks the deployer configures; it does not enforce storage duration. Ship to S3 with Object Lock, Loki with retention, Splunk, or an equivalent store set to at least six months.

Article 12 versus Article 26(6). Article 12 is the design-time obligation on the provider to make a high-risk system technically capable of automatic logging. Article 26(6) is the runtime obligation on the deployer to keep those logs. Pipelock contributes evidence toward both: it generates structured logs that support the Article 12 capability requirement, and it emits those logs to the retention sink the deployer operates in support of the Article 26(6) six-month floor. Pipelock does not by itself satisfy either obligation; the deployer's program does.

Sample retention setup

Minimal emit configuration paired with a retention-controlled sink:

```
emit:
  webhook:
    url: https://logs.example.invalid/ingest
    min_severity: info
  syslog:
    address: udp://syslog.example.invalid:514
    min_severity: info

# Pair with one of these on the storage side, set to >= 6 months:
#   - AWS S3 + Object Lock (compliance mode) with 6-month retention rule
#   - Google Cloud Storage with retention policy >= 6 months
#   - Azure Blob immutable storage with 6-month retention
#   - Grafana Loki with retention configured >= 6 months
#   - Splunk index lifecycle policy >= 6 months
# Sector law (financial services internal-governance rules, GDPR) may
# require longer retention. Configure the storage side to the longest
# applicable rule.
```

What Pipelock does not cover

- Article 9 risk-management process (organisational), Article 10 training-data governance, Article 11 technical documentation (system level).
- Article 27 fundamental rights impact assessment.
- Article 43 conformity assessment and certification.
- Conditional paragraphs 7-12 of Article 26 (workplace notice, public-authority registration, GDPR DPIA linkage, post-remote biometric identification, notice to natural persons affected by Annex III decisions, authority cooperation). Check the full OJ text and qualified legal advice.

Source: Regulation (EU) 2024/1689, Article 26. Official Journal text: eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202401689

When the obligations apply: Regulation (EU) 2026/1744, the Digital Omnibus on AI, amends Regulation (EU) 2024/1689. It was published in the Official Journal on 24 July 2026 and entered into force on 27 July 2026. Annex III stand-alone high-risk obligations apply from 2 December 2027. Annex I embedded-in-product safety-component obligations apply from 2 August 2028. Article 5 prohibited practices have been in force since 2 February 2025.

Amendment history. The European Parliament endorsed Regulation (EU) 2026/1744 on 16 June 2026 and the Council gave final approval on 29 June 2026. It is the first major amendment to Regulation (EU) 2024/1689. Earlier versions of this matrix cited the pre-amendment high-risk date, which this amendment superseded.

Framing. *Pipelock supplies runtime evidence inside the deployer's existing compliance programme. Pipelock does not "solve" or "satisfy" the EU AI Act. The Article 12 framing is "provides evidence toward the technical-capability requirement," not "satisfies it."*

Full mapping: pipelab.org/learn/eu-ai-act-compliance/