

Sentinel Evidence Pack

Project	sentinel-cli
Sovereign scope	local
Data residency	local
Storage backend	sqlite
Generated (UTC)	2026-04-16T23:34:37+00:00
Since	—
Until	—

This evidence pack is produced by the Sentinel decision trace and policy enforcement layer. It documents Art. 12 / 13 / 14 / 17 technical controls. It does **not** replace risk management, data governance, conformity assessment, or post-market monitoring.

Executive summary

Traces in window	0
ALLOW	0
DENY	0
EXCEPTION_REQUIRED	0
Human overrides	0
Unique agents	0
Unique policies	0
Truncated	no

EU AI Act coverage

```
=====
EU AI ACT COMPLIANCE REPORT
Generated: 2026-04-17T01:34:37
Overall: PARTIAL
Automated coverage: 36%
Days to enforcement (2 Aug 2026): 107
=====

[PART] Art. 9 (auto) – Risk management
No PolicyEvaluator configured. In production, wire a SimpleRuleEvaluator or
LocalRegoEvaluator.
→ Configure a PolicyEvaluator on Sentinel

[TODO] Art. 10 (manual) – Data governance
Data governance is not automatable by a middleware kernel.
→ Document your training/evaluation data provenance, quality, and bias mitigation

[TODO] Art. 11 (manual) – Technical documentation
Annex IV technical documentation is a human deliverable.
→ Prepare Annex IV technical documentation

[OK ] Art. 12 (auto) – Automatic record keeping
Every wrapped call produces a DecisionTrace automatically, stored append-only.

[OK ] Art. 13 (auto) – Transparency & information to deployers
Traces record agent, model, policy name/version, and result per decision.

[OK] Art. 14 (auto) – Human oversight
Kill switch implemented; every override recorded as linked trace entry.
→ Define who operates the kill switch

[TODO] Art. 15 (manual) – Accuracy, robustness, cybersecurity
Model evaluation and adversarial testing are outside the trace layer.
→ Run model evaluation suite and penetration tests

[OK ] Art. 17 (auto) – Quality management system
Continuous, append-only trace record satisfies the traceability requirement.
→ Document the full QMS – not only traceability

[PART] Art. 16 (auto) – Provider obligations
Art. 16(d) deployer logging and 16(f) post-market monitoring evidence are produced
automatically via the trace store.
→ Complete provider registration, conformity assessment, CE marking

[PART] Art. 26 (auto) – Deployer obligations
Art. 26(5) deployer logging and Art. 26(6) human oversight primitives are shipped (kill
switch + trace store).
→ Document oversight procedures, train staff, wire incident reporting

[PART] Art. 72 (auto) – Post-market monitoring (GPAI)
Records model identity, inputs hash, outputs and decision chain for any GPAI call – the raw
evidence Art. 72 requires.
→ Publish a GPAI post-market monitoring plan (only if you deploy GPAI as high-risk)

=====
```

Trace samples

No traces in the selected window.

Hash manifest

The evidence pack digest is a SHA-256 of the trace hash list. Recompute it from the NDJSON export of the same window to verify this pack covers the same traces.

Pack digest: e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855

No hash entries — empty trace window.

Sovereign attestation

Self-contained governance attestation. The attestation hash is a SHA-256 of the document content (sorted keys). Verifiable offline with *sentinel attestation verify*.

```
{
  "attestation_hash": "5dcb81b7811e51ed8de5add9623e31bd441b1d495f94f2313c4343e7ead965b4",
  "compliance_summary": {
    "automated_coverage": 0.36363636363636365,
    "days_to_enforcement": 107,
    "overall": "PARTIAL"
  },
  "data_residency": "local",
  "generated_at": "2026-04-16T23:34:37.751041+00:00",
  "kill_switch_active": false,
  "project": "sentinel-cli",
  "schema_version": "1.0.0",
  "sentinel_version": "3.3.0",
  "sovereign_scope": "local",
  "sovereignty_assertions": [
    "apache-2.0-licensed",
    "zero-us-cloud-act-in-critical-path",
    "air-gap-capable",
    "tamper-resistant-trace-schema"
  ],
  "storage_backend": "sqlite",
  "title": "Sentinel Governance Attestation",
  "trace_count": 0
}
```

Dependency sovereignty scan

Packages scanned: 115. Sovereign: 113. US-owned: 3. Unknown: 85. Sovereignty score: 98%.
Critical-path violations: 0.

*This pack documents Art. 12 / 13 / 14 / 17 technical controls only. Run `sentinel audit-gap` to see the deployment and organisational obligations that remain. Pilot or BSI-pre-engagement enquiries are tracked publicly on GitHub: github.com/sebastianweiss83/sentinel-kernel/issues — label **pilot**.*