

Sentinel Evidence Pack

Project	sentinel-pilot
Sovereign scope	local
Data residency	local
Storage backend	sqlite
Generated (UTC)	2026-04-16T16:12:41+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	10
ALLOW	0
DENY	0
EXCEPTION_REQUIRED	0
Human overrides	0
Unique agents	1
Unique policies	0
Truncated	no

EU AI Act coverage

```
=====
EU AI ACT COMPLIANCE REPORT
Generated: 2026-04-16T18:12:41
Overall: PARTIAL
Automated coverage: 36%
Days to enforcement (2 Aug 2026): 108
=====

[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

trace_id	agent	result	started_at
088e5614-39a...	approve_expense	—	2026-04-16T16:12:41+00:00
75bbdd8f-c80...	approve_expense	—	2026-04-16T16:12:41+00:00
d1128a2d-2ed...	approve_expense	—	2026-04-16T16:12:41+00:00
8a25b95c-438...	approve_expense	—	2026-04-16T16:12:41+00:00
9e858eca-b6d...	approve_expense	—	2026-04-16T16:12:41+00:00
8198008e-f44...	approve_expense	—	2026-04-16T16:12:41+00:00
9e9652c3-7b4...	approve_expense	—	2026-04-16T16:12:41+00:00
02763bc0-cab...	approve_expense	—	2026-04-16T16:12:41+00:00
dcaf7a46-7e3...	approve_expense	—	2026-04-16T16:12:41+00:00
7d2ad7e0-3bc...	approve_expense	—	2026-04-16T16:12:41+00:00

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: a43040b4408e77216001de65fcd3b634b28c62dadad10859325e3d2ba00f7d76

```
088e5614-39a7-4cad-a7fe-e0a4a48d63a5
inputs=7ff72c7d4af6489258f5c0c4cdf283df30838260b0a1063216cc747c214e7af2
output=8722b326c24b41739ca55cde1855ed55ee94af4cffed03f8d3be58a9f895cc03
75bbdd8f-c80a-414c-901a-dc10239904ad
inputs=b0e582bea39f1f2c242b115f4376fcd60601e51ae55b1180a8e77904b65e4478
output=5c3fadb90b45f4a86cf7alee92b070f13e01245218ed0b294deeeb8f6c6ef942
d1128a2d-2ed9-4f59-afff-5db3812ee2f1
inputs=1d299fa10b3d648a8bf7fd809ad57e3247c86f1b47f7101ecfeb1841dd1b637a
output=9597290fab450a6bc58d142e9b3dc905c869a344f0dbcbc8b50b9e04135f99c1
8a25b95c-4383-4952-a36d-ed8513edaf1c
inputs=560d31353a8e7dc8c17d4a53ae937b2bc98202d36d011dc5b4edc18021ddc4b5
output=eb0a5695e57569bc164277227951cd3777caaf0bacd1eba3cd0be9de48d1c262
9e858eca-b6dd-4cf9-ba8b-685fa4eb2af5
inputs=53b229cece108f67de9de0a310494c0948d8e11435cf4c13a741b3e77d6ac1af
output=d572099d3f0c549288ac903e041c3fc6b03d8da94f90599df543912cc19e9acc
8198008e-f445-4d18-a768-84d73e93e1cf
inputs=e5ccbfeaa9a073be033352a2c70ae462e598efb5b6b3b371d167983c8d512b76
output=9597290fab450a6bc58d142e9b3dc905c869a344f0dbcbc8b50b9e04135f99c1
9e9652c3-7b44-4185-b87e-bb90d5b63519
inputs=39df5987ee8ddb9b63d75bf5753a7ed51eb01967c6a0bb9a86eb93328ed310fc
output=9597290fab450a6bc58d142e9b3dc905c869a344f0dbcbc8b50b9e04135f99c1
02763bc0-cabb-4abe-8cf5-697536bf469a
inputs=09797a984793d55a41d5c492ca347ac48aaf07603c8b1b950e8b7e2e50f8b65f
output=34458f4783e02e214d08db5bca47fac17403fd6f8ceddcadac610d0548f17b69c
dcac7a46-7e3c-4884-9da5-49f1f22b9dda
inputs=3573d623c6a952e7592705da2195bf2414a3a9fd47ab05b86be261b28e0e342a
output=31c7cae62542e2cd80cea3410195510e831969a84179922519b409a6f36ba3da
7d2ad7e0-3bc6-40e6-944a-8b83eff4e4d9
inputs=93bbbedcca8d0eb04b6a87ba850ed0e951364c8447bd96d0d8d6abf7ecc8cf9c2
output=1c006966ad743eace4f691e21a7c9f420ca84b732bfd033f4d5a0f8aa66fba67
```

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": "380cc9fa46457509d779248bb35064110d08c1d9f2dae1b92314376e2b4d39a9",
  "compliance_summary": {
    "automated_coverage": 0.36363636363636365,
    "days_to_enforcement": 108,
    "overall": "PARTIAL"
  },
  "data_residency": "local",
  "generated_at": "2026-04-16T16:12:41.504268+00:00",
  "kill_switch_active": false,
  "project": "sentinel-pilot",
  "schema_version": "1.0.0",
  "sentinel_version": "3.2.0",
  "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": 10
}
```

Dependency sovereignty scan

Packages scanned: 17. Sovereign: 17. US-owned: 1. Unknown: 10. Sovereignty score: 100%. 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**.*