EU AI Act

Compliance assessment — 2024/1689

Server: Kroger

Slug: kroger
Scan id: 0331f470-e371-4188-b1aa-cbc79c57f686

Assessed at: 2026-05-24 07:20:56 UTC
Sentinel version: 0.4.0
Rules version: 2026-04-23

' Non-compliant

DRAFT for review — not legal advice. See attestation block for verification instructions.

Table of contents

1. Executive summary

Assessment of Kroger against EU AI Act: overall status non compliant. Of 5 controls, 4 met, 1 unmet, 0 partial, 0 not applicable. 5 control(s) fell within MCP Sentinel's current assessor coverage; remaining control(s) are documented as not_applicable until Phase 6 expands coverage. Unmet controls have findings at or above the framework's mandatory severity threshold and should be remediated before relying on this server in a regulated deployment. All claims are traceable to individual finding rows via finding_id and to the governing rule via rule_id; the enclosing signed envelope commits MCP Sentinel to the exact bytes of this report.

2. Coverage & transparency

Coverage band: low

Coverage ratio: 40%

Rules version: 2026-04-23

Analysis techniques applied:

- ast-taint
- capability-graph
- entropy
- linguistic-scoring
- schema-inference

3. Controls summary

Control	Name	Status	Evidence
Art.9	Risk Management System'	Unmet	1
Art.12	Record-Keeping'	Met	0
Art.13			

Transparency & Provision of Information to Deployers' Met 0
Art.14Human Oversight' Met 0
Art.15 Accuracy, Robustness, and Cybersecurity' Met0

4. Control details

Art.9 — Risk Management System

' Unmet

22 assessor rule(s) evaluated this control; 1 finding(s) observed (1 critical); at least one finding is at or above the high threshold (status: unmet).

Evidence:

[Critical] D5 (finding 454c19bd-2e41-43e5-9462-8c0854bf615b, confidence 80%)

SOURCE: external-content at npm:modelcontextprotocol@0.1.0 — The advisory at https://socket.dev/blog/typosquat-mcp-sdk-wave identifies "modelcontextprotocol" as a confirmed malicious package: 2025 — u

Required mitigations:

- Remove the flagged package immediately. Regenerate the lockfile from scratch. Audit the build environment (CI runners + developer machines) for artifacts the package may have written during install — stolen credentials, persistence hooks, or outbound network connections. Rotate every secret the build environment had access to. Report the package to the registry's security team if it is not already taken down.

Art.12 — Record-Keeping

' Met

5 assessor rule(s) evaluated this control; no findings observed.

Art.13 — Transparency & Provision of Information to Deployers

' Met

14 assessor rule(s) evaluated this control; no findings observed.

Art.14 — Human Oversight

' Met

13 assessor rule(s) evaluated this control; no findings observed.

Art.15 — Accuracy, Robustness, and Cybersecurity

' Met

111 assessor rule(s) evaluated this control; no findings observed.

5. Multi-step attack chains

No multi-step attack chains were synthesized for this server.

6. Cryptographic attestation

Algorithm: HMAC-SHA256
Key ID: mcp-sentinel-dev
Signer: mcp-sentinel/v1
Signed at: 2026-05-24T11:15:45.556Z
Canonicalization: RFC8785

HMAC-SHA256 signature (base64, wrapped at 64 chars):

```
P/9o/6juBo6m/euhz9HzdHs9y3UPsQ1AJLilH6DJ2+o=
```

Verification instructions:

```
To verify this report:
  1. Extract the report body (everything except the .attestation field).
  2. Canonicalize the body via RFC 8785 (JCS).
  3. Compute HMAC-SHA256 with the signing key for key_id "mcp-sentinel-dev".
  4. Base64-encode the result and compare with the signature above.
```