

PRACTITIONER CHECKLIST

EU AI Act Article 12 Compliance Checklist

A practical, self-assessment checklist covering scope determination, the logging requirements Article 12 actually demands, the tamper-evidence properties your records must have, and the independent verifiability test regulators apply. Based on Article 12 and Article 99 of the EU AI Act, current following the Council's final adoption of the Digital Omnibus on 29 June 2026.

Where things stand: Article 12 becomes enforceable for Annex III high-risk systems on 2 December 2027. Article 50 transparency obligations are live now, from 2 August 2026. Article 12 doesn't reset just because the enforcement date moved, it requires logging across the system's operational lifetime, so starting now still determines how complete your evidence trail is when enforcement begins.

1. Are you in scope?

Article 12 applies to high-risk AI systems under Annex III. If your AI system falls into any category below, Article 12 applies to you.

- | | |
|--|--|
| ☐ Credit scoring, fraud detection, AML/KYC automated review | ☐ CV screening, candidate scoring, promotion recommendation |
| ☐ Clinical decision support, diagnostic imaging, triage | ☐ Automated assessment, student evaluation systems |
| ☐ Risk assessment tools in criminal proceedings | ☐ AI systems managing essential/critical infrastructure |
| ☐ Real-time or post-hoc biometric identification | |

If you checked any box above, the sections below apply to your organisation.

2. The 12 logging requirements

Practical requirements derived from Article 12(1) and 12(2). Check off what your current logging already satisfies.

- ☐ **Automatic generation.** Logs are created at the moment of each decision, not assembled or reconstructed afterward.

- ☐ **Full decision context captured.** Every record includes the AI input, output, model identifier, and decision context.
- ☐ **Policy evaluation recorded.** Each decision is tested against governing policy, and the result is stored alongside the decision.
- ☐ **Six-month minimum retention.** Records are retained for at least six months from the point of generation.
- ☐ **Post-hoc reconstruction possible.** Logs are sufficient to reconstruct how and why the system operated.
- ☐ **Available to regulators on request.** Records can be produced for national competent authorities without manual assembly.
- ☐ **Biometric-specific fields, where applicable.** Start/end time of use, reference database, and individuals involved are captured for biometric identification systems.
- ☐ **Tamper-evident structure.** Records are written so that modifying any entry is mathematically detectable, not just logged to a mutable database.
- ☐ **Independently bound timestamp.** The time of capture is cryptographically bound to the record, not self-reported by the application.
- ☐ **Verifiable without vendor access.** Chain integrity can be checked by a third party without needing your platform or vendor's cooperation.
- ☐ **On-demand export.** A complete, verifiable audit package can be produced on request, suitable for regulators, auditors, or courts.
- ☐ **Built in, not documented only.** The logging capability is technical, part of the system itself, not a policy statement describing intent to log.

3. Tamper-evidence property checklist

A log that can be edited is a statement, not evidence. These are the properties that make a record stand on its own.

- ☐ Records are cryptographically sealed at the point of capture, not after the fact.
- ☐ Records are hash-chained (e.g. SHA-256): modifying any single record breaks every hash after it.
- ☐ Timestamps come from a trusted third-party time authority (e.g. RFC 3161), not the application itself.
- ☐ Tampering is detectable without needing the vendor's systems, dashboard, or cooperation.
- ☐ Chain integrity is mathematically provable, not asserted by policy or contract language.

4. The independent verifiability test

The most frequently overlooked Article 12 criterion. Ask these four questions about your current evidence trail.

- ☐ Can an auditor, regulator, or court verify a record's integrity without logging into your platform?
- ☐ Can verification be done with standard, publicly available tools, not proprietary vendor software?
- ☐ Does verification require an API call or an account? If yes, that is a single point of failure.
- ☐ Would the evidence still hold up if the vendor were acquired, shut down, or unreachable?

Checked more boxes on the left than the right?

That gap is exactly what the Umbra Trust Protocol closes: automatic capture, hash-chained tamper-evidence, RFC 3161 timestamping, and independent verification with standard tools, no account required.

We'll walk through your specific gap in a 30-minute evidence briefing, no commitment required.

[BOOK AN EVIDENCE BRIEFING →](#)