

EU AI Act Article 12: a practical starting checklist

Article 12 requires high-risk AI systems to **technically allow automatic recording of events over their lifetime**, with traceability an outsider can rely on. These six questions surface most of the work.

1 · What counts as an “event” in your system?

Inventory the decisions, not the log lines: approvals, denials, escalations, abstentions, human overrides. If a decision matters enough to defend, it matters enough to record.

2 · Is the recording automatic and unskippable?

A logging path that engineers can disable, or that fails silently, fails the “technically allow automatic recording” test at exactly the wrong moment.

3 · Could the record be edited without detection?

If yes, the record is testimony, not evidence. Seal it — hash chains are cheap; rebuilding credibility isn't.

4 · Who vouches for the timestamps?

If the answer is “we do,” anchor to an independent authority. RFC 3161 exists for this; public timestamp authorities cost nothing.

5 · How long do you keep it — really?

Six months is the statutory floor. Limitation periods, sector rules, and product-passport regimes usually mean product-lifetime-plus.

6 · Can an outsider check a record without your help?

The final exam. If verification requires your servers, your goodwill, or your continued existence, it will be discounted precisely when it matters most.

The property behind all six: a record that *proves* rather than *asserts* — automatic, lifetime, tamper-evident, independently time-anchored, attributable, reproducible, and honest about refusals. That is the kind of record Corobate receipts are built to be: sealed, anchored to public RFC 3161 authorities, and verifiable by anyone in a browser at corobate.com/verify.