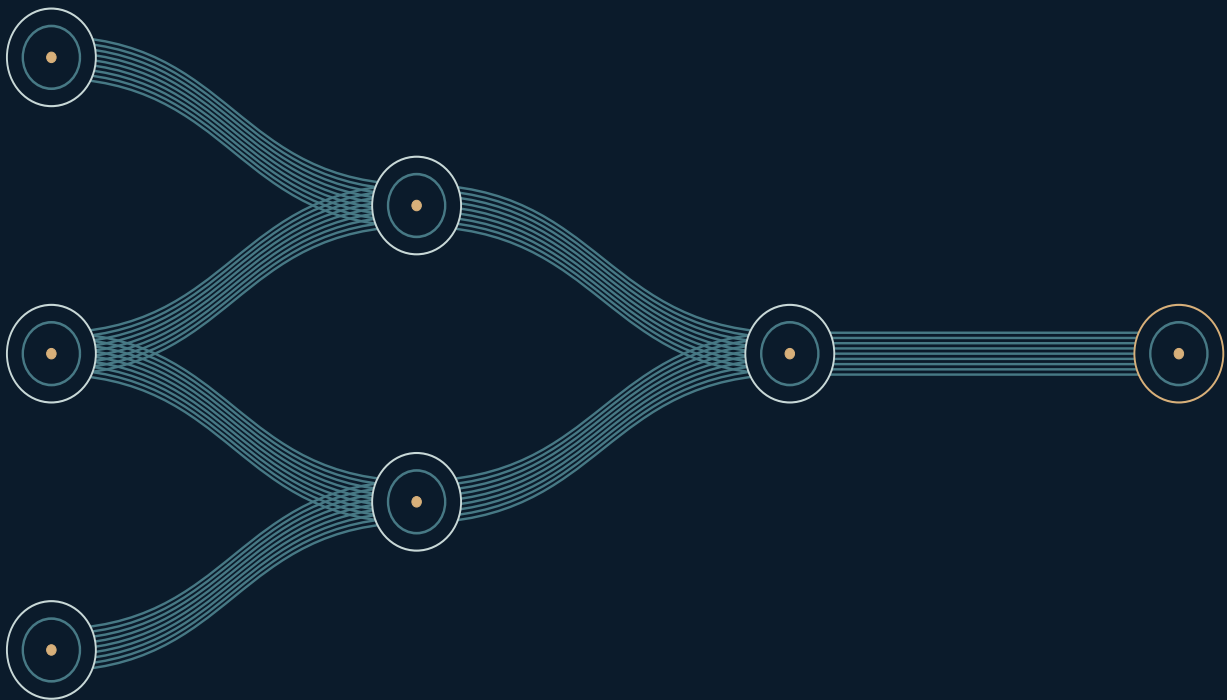




ENGINEERING / OCTOBER 2026

Build a memory for consequential decisions

Why AI assurance depends on evidence lineage, recorded authority and recoverable context



THE DECISION IN BRIEF

A useful AI decision record makes a disputed outcome reconstructable: what evidence existed, who authorised the action and what actually happened, including any missing link.

- 01

Build the record around a real reconstruction question. A source withdrawal should lead to potentially affected cases, the human judgement and the downstream decision.
- 02

Keep provenance, integrity and correctness distinct. An unaltered, well-attributed record may still contain a false claim or an unauthorised action.
- 03

Retain the smallest controlled evidence set that supports review and remediation. Test whether an independent colleague can reconstruct the case before buying a broader logging architecture.

THE MAYDEN VIEW

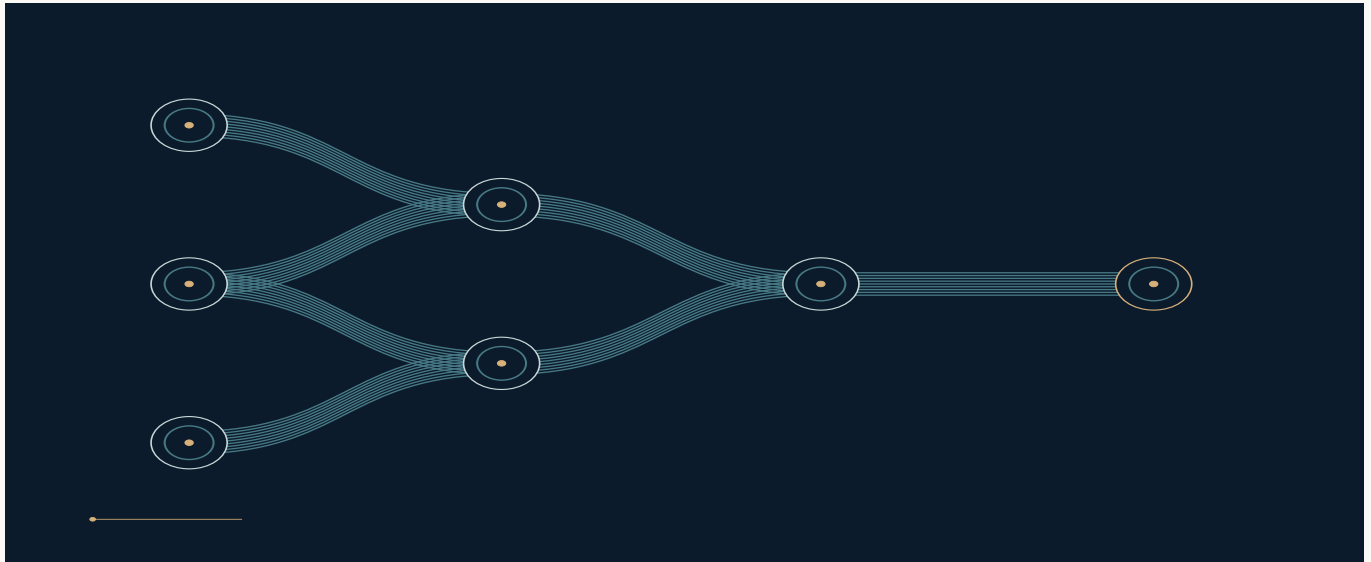
The decisive test of a record is whether it can explain the challenged decision.

INSIDE THIS PERSPECTIVE

The argument at a glance	3
01 / Start with the challenged decision	4
Exhibit 01 / A withdrawn certificate should lead to the affected decision	5
02 / Link evidence to authority and action	6
Exhibit 02 / Three kinds of confidence require different evidence	7
03 / Retain the smallest useful record	8-9
Exhibit 03 / Reconstruction requires different evidence from regeneration	10
04 / Prove reconstruction in a case	11
The leadership agenda	12
Method and references	13

ONE DECISION, FOUR CONNECTED QUESTIONS

Reconstruct the decision



PROVENANCE CHAIN / CONCEPTUAL ARTWORK

01 Start with the challenged decision

Start with the decision somebody may challenge

02 Link evidence to authority and action

Record observable evidence, not inferred reasoning

03 Retain the smallest useful record

Retain enough to reconstruct, with controlled access

04 Prove reconstruction in a case

A withdrawn certificate reveals the missing decision link

The decisive test of a record is whether it can explain the challenged decision.

CHAPTER 01

01

Start with the challenged decision

Start with the decision somebody may challenge

A supplier certificate is withdrawn after an AI-assisted review. Which decisions used it? Did a specialist rely on its disputed claim? Did any authorised action follow? A dashboard of successful model calls cannot answer those questions without links to the evidence, review and business record. The executive requirement is a reconstructable decision, with missing evidence left visible.

Re-running today's model on today's documents answers a new question. It does not establish what an analyst knew when the original decision was made. In the illustrative supplier review, the relevant record preserves the certificate version, unresolved gaps, specialist judgement and the state changed by procurement.

mayden proposes treating the decision receipt as a business artifact. It should be readable enough for an accountable manager and precise enough for technical investigation. The receipt links to underlying evidence rather than reproducing everything in one document. This reduces duplication and makes access controls manageable. Its design begins with the questions a reviewer or affected person needs answered, not with whatever events happen to be easiest for a software library to emit.

Do not confuse provenance with truth

W3C's PROV data model represents entities, activities and responsible agents and the relationships among them. ^[1] It provides a useful vocabulary for describing how an output was produced. mayden's application is to connect a decision to source versions, extraction steps, model calls, policy checks and human actions. A source can then be traced through several transformations without treating all those transformations as equivalent evidence.

Three properties require separate treatment. Provenance concerns origin and process. Integrity concerns whether a record has changed under the applicable verification method. Correctness concerns whether a claim or action is justified. An unaltered record can contain an error. A correctly attributed document can be outdated. A faithful log of an unauthorized action is useful evidence of a failure. Combining these properties into a single trust indicator gives decision-makers false reassurance.

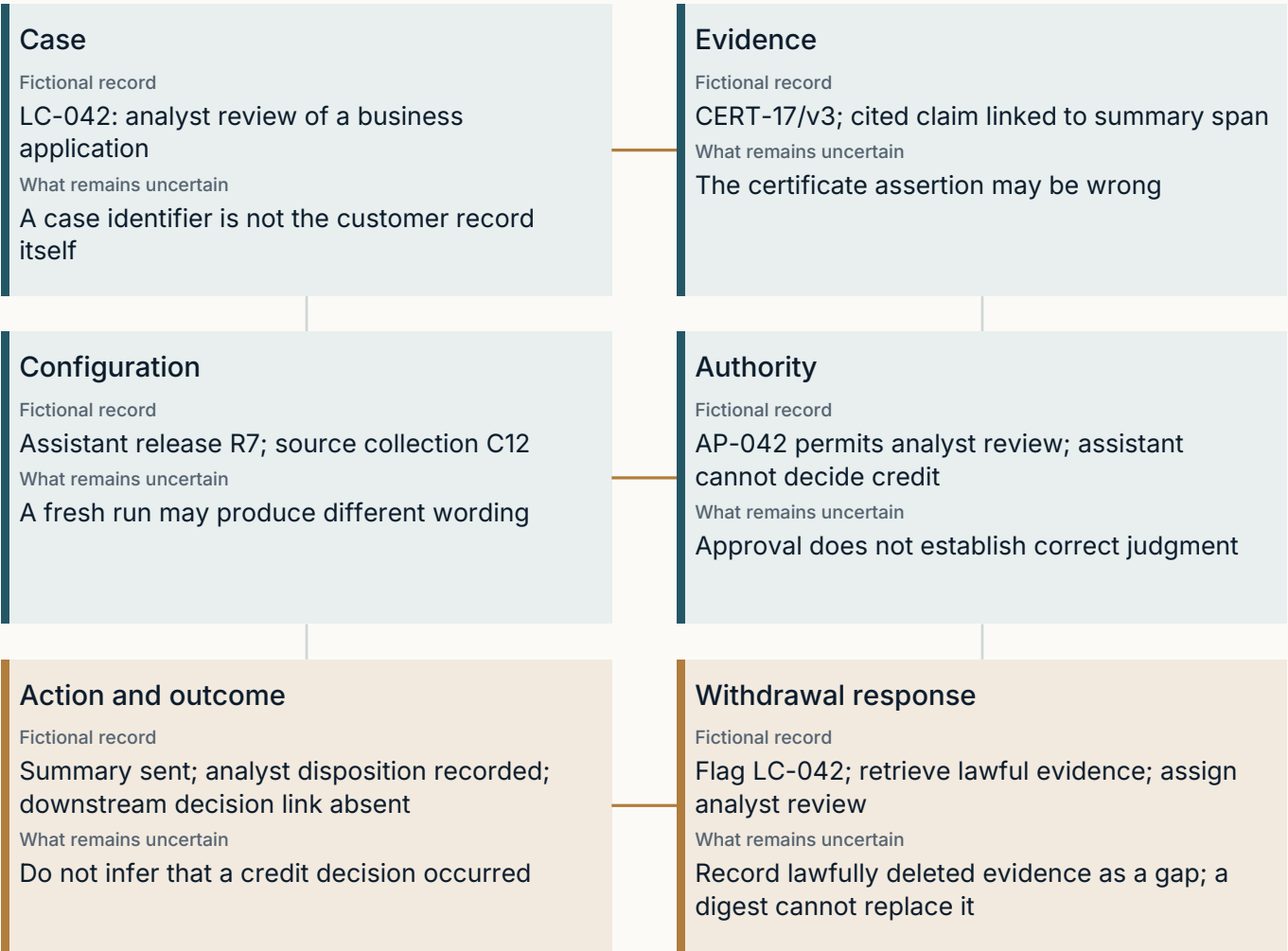
Preserve the type of each statement. A quoted source assertion, an analyst inference and a management assumption may all appear in the same report, but they should not share an undifferentiated evidence label. Record contradictions and unsupported gaps. If the source changes, the organization should be able to locate dependent decisions for review. This is a proposed operational use of lineage, not a claim that every dependent decision must automatically be reversed.

ILLUSTRATIVE DECISION TOOL

A withdrawn certificate should lead to the affected decision

Synthetic receipt; no customer or institution data

RECEIPT LINKS / CONNECTIONS DO NOT ESTABLISH THE MISSING DECISION



THE MANAGEMENT IMPLICATION

A missing decision link is an investigation gap, not permission to generate a plausible history.

Identifiers and events are invented. Source access, retention and deletion rules remain applicable. This is not a legal sufficiency standard. Sources: [1], [3], [4]

CHAPTER 02

Link evidence to authority and action

02

Record observable evidence, not inferred reasoning

Generated explanations can be useful to readers, but they should not be treated as a complete causal account of a model's behavior. Research on chain-of-thought faithfulness showed that biasing inputs could influence answers without being disclosed in the generated explanation. Those experiments used historical models and particular tasks. ^[2] Their practical lesson is that a plausible narrative does not substitute for recorded inputs, actions and checks.

Retain the evidence the organization can observe: the request, permitted scope, relevant source identifiers, configuration version, tool request, policy decision and downstream response. Where prompts contain sensitive data, use controlled references and a proportionate retention design. Record a human reviewer's decision separately from the system's proposal. A reviewer may accept a result for a reason that the model did not express, or may override it based on information that never entered the model context.

Be precise about replay. A captured configuration may support reconstruction without guaranteeing byte-identical model output. Hosted providers can change infrastructure, nondeterministic computation can affect results and an external API's state can evolve. A replay mode should identify which dependencies are preserved and which are simulated or unavailable. The most credible record states these limits. Claiming perfect reproducibility where none exists weakens the usefulness of the entire evidence chain.

Connect the receipt to authority and business state

mayden's proposed receipt contains six linked elements: case, evidence, configuration, authority, action and outcome. The case identifies the business question and relevant object. Evidence names exact source versions and limitations. Configuration identifies the deployed system. Authority records the permission or approval. Action captures the attempted change. Outcome captures the observed business state, including uncertainty. This is an original design pattern intended for local adaptation.

Software supply-chain provenance offers a useful analogy. The SLSA v1.2 build-provenance schema separates build inputs and dependencies from details of a particular build execution. ^[3] An AI service can similarly distinguish a reusable workflow definition from a specific decision run. The analogy has limits: business evidence and human judgment are broader than software builds. Organizations should borrow the separation of concerns without claiming that an existing build attestation proves the legitimacy of a business decision.

Use stable identifiers to connect systems. A customer case, a model request and a transaction may have different native identifiers; the receipt needs explicit links. Capture time and ordering with enough precision for the process, and distinguish event time from ingestion time. Store the record close enough to the action that missing receipts become detectable. An optional logging step after successful execution leaves a gap exactly when a crash or interruption makes the record most valuable.

MAYDEN FRAMEWORK

Three kinds of confidence require different evidence

Evidence distinctions

Provenance	What it can establish Where an item came from	What it cannot establish Whether the underlying claim is true
Integrity	What it can establish Whether a recorded item changed	What it cannot establish Whether the original item was correct
Decision support	What it can establish Whether evidence justifies a choice	What it cannot establish That future conditions will be identical
THE MANAGEMENT IMPLICATION A signed record should not be presented as a truth certificate.		

mayden synthesis. Cryptographic verification is bounded by keys, implementations and trust assumptions. Sources: [1], [5], [6]

CHAPTER 03

03

Retain the smallest useful record

Retain enough to reconstruct, with controlled access

NIST's log-management guidance emphasizes both infrastructure and organizational processes. ^[4] Retention, access, monitoring and review are part of the design. An organization that records everything indefinitely may increase privacy and security exposure while making investigations harder. Define the purpose of each retained field and the questions it must support. Separate high-value decision evidence from verbose diagnostic traces that can expire sooner.

Article 12 of the EU AI Act illustrates the distinction between an indiscriminate transcript and purpose-led records. For systems within the relevant high-risk scope, it requires technical logging capabilities that support risk identification, post-market monitoring and operational oversight. ^[8] It does not turn every conversation with an AI system into the same legal record. Classification, role and applicable dates still determine the obligation.

Design the receipt from the reconstruction question backward. To identify affected customers after a source is withdrawn, the organization needs the source version, the decisions that used it and the downstream action references. Retaining every token is neither a

substitute for those links nor always appropriate. mayden proposes testing whether a controlled reviewer can answer that question from the retained record, with access controls and deletion rules still enforced.

Certificate Transparency's experimental RFC describes append-only logs and Merkle proofs for checking inclusion and consistency. ^[5]

These concepts can inform integrity design, but a business decision ledger is a separate system with its own trust assumptions. A digest can detect that the retained bytes differ from a recorded reference; it cannot prove the original document's claims. Decide who can write records, who can alter retention policy and how independent checks would reveal tampering or gaps.

C2PA's specification defines signed content provenance and assertions. ^[6] In an enterprise evidence process, such credentials can help establish aspects of a content object's history where supported. They do not remove the need to assess its substance. Record credentials as one evidence feature alongside source authority, date and relevance. Do not penalize a legitimate source solely because it lacks a credential. Absence of a particular provenance mechanism is an uncertainty about history, not proof of falsehood.

CHAPTER 03

03

Retain the smallest useful record

Earn the record's cost through a concrete investigation

A detailed evidence graph can consume engineering time without improving an investigation. Start with one consequential workflow and the questions operators cannot currently answer. Collect the minimum links that resolve them. More logging is justified only when another reconstruction or remediation task requires it.

Dataset documentation offers another discipline. Datasheets for Datasets proposes recording motivation, composition, collection and intended use. ^[7] A decision system can reuse that documentation at the dataset level instead of copying it into every receipt. Each run can

reference the relevant version. This makes evidence more economical and preserves context. It also creates an explicit owner who can correct documentation when the underlying data changes.

The business case should include shorter investigations, more targeted remediation and better change impact analysis. These are hypotheses to measure, not benefits assumed in advance. Compare the time required to resolve representative cases before and after the receipt design. Ask whether investigators can locate affected decisions when a source is withdrawn. If the record cannot answer a concrete operational question, reconsider its fields and interface before investing in a broader architecture.

ILLUSTRATIVE SCENARIO

Reconstruction requires different evidence from regeneration

mayden proposed review design

What was available?	Retained evidence Exact source versions and missing-evidence flags	Remaining limit Source assertions may be wrong
What was permitted?	Retained evidence Policy version and action-specific approval	Remaining limit Approval may itself be mistaken
What happened?	Retained evidence Downstream state and event links	Remaining limit External events may remain unavailable
Would it happen again?	Retained evidence Preserved configuration and dependencies	Remaining limit Replay need not be byte-identical
THE MANAGEMENT IMPLICATION A useful receipt separates the historical record from a fresh model-generated explanation.		

Original synthesis. No claim of perfect reproducibility or legal sufficiency. Sources: [1], [2], [3]

CHAPTER 04

04

Prove reconstruction in a case

A withdrawn certificate reveals the missing decision link

Consider a fictional lender using an assistant to summarize business documents for an authorized analyst. The assistant cites a supplier certificate that is later withdrawn. The institution now needs to know which case summaries used that version, whether the analyst relied on the disputed claim and whether a subsequent decision changed the exposure. A list of model requests does not answer those questions unless it connects to the source, the review and the downstream business record.

Exhibit 01 gives this fictional case a small, linked receipt. The certificate version and cited summary span identify the evidence used; the configuration identifies the system; a separate approval record identifies the analyst and permitted action. In the illustration, the downstream decision link is absent. The correct finding is therefore that the assistant produced a reviewed summary, while any later credit action remains unestablished. A withdrawal should flag linked cases for review, not automatically reverse every decision. Independent supporting evidence may make the withdrawn claim immaterial in some cases.

Test this design with a synthetic withdrawal in a controlled environment. Ask an independent reviewer to find the potentially affected cases, distinguish proposals from completed decisions and explain which evidence remains unavailable. Measure investigation effort and missed links against the current process. No improvement is assumed here. The exercise may reveal that document identity is reliable but human overrides are poorly recorded, in which case investing in a more elaborate model trace would address the wrong gap.

Choose the smallest controlled evidence set that supports the review. Indefinite prompt retention may add exposure without resolving the case; a digest alone may identify bytes while leaving their substance unavailable. Keep necessary source access, authority and action links under explicit retention rules, and expose any dependency that cannot be recovered.

Test reconstruction before expanding the architecture

Before release, ask a colleague outside the delivery team to reconstruct an approved action, a rejected proposal, a human override and an uncertain outcome. They should identify the evidence, authority and observed result without interviewing the engineer. Record each missing link. The exercise tests whether the receipt answers the business question, rather than whether software emits enough events.

After release, sample receipts and verify their source and action links. Exercise permissions, retention changes and deletion through the connected systems. A lawful deletion may leave evidence unavailable; the receipt must state that limitation rather than imply complete replay. Protect confidential material while preserving the context an authorised reviewer needs.

Start with the case the organisation currently struggles to explain. Measure reconstruction time, unresolved links and the ability to find potentially affected decisions when evidence changes. Add fields only when they support those tasks. The CEO should receive a concise account of what was known, allowed and observed - and what still cannot be established.

FROM INSIGHT TO ACTION

Decisions to take forward

BUSINESS DECISION OWNER

Record missing links as gaps; reject generated history as evidence.

Evidence to require: Disputed-case receipt linking source, authority, action and outcome

DATA AND RECORDS OWNERS

Keep the smallest lawful evidence set that supports review.

Evidence to require: Access, retention and deletion treatment for underlying sources

INDEPENDENT REVIEWER AND OPERATIONS

Repair the link preventing reconstruction before adding trace volume.

Evidence to require: Synthetic withdrawal exercise and affected-case list

mayden connects senior judgement, research and engineering to turn strategic choices into working capabilities.

EVIDENCE YOU CAN INSPECT

Research notes

Method and boundaries

Narrative synthesis of eight primary research and technical specifications accessed 10 October 2026, combined with a proposed mayden receipt architecture.

Provenance models, explanation faithfulness, software provenance, security logging, transparency logs, content credentials and dataset documentation.

No claim of legal sufficiency, forensic certification or perfect replay. RFC 9162 is an experimental certificate protocol; C2PA concerns content credentials. Their application to business decisions is an explicitly labeled analogy.

Primary sources and author research

[1] PROV-DM: The PROV Data Model

W3C / 2013-04-30. Overview; entities, activities and agents. A provenance data model for describing entities, activities and agents; recording these relationships does not prove that a decision or its inputs are correct.

[Read the source](#)

[2] Language Models Don't Always Say What They Think: Unfaithful Explanations in Chain-of-Thought Prompting

Turpin et al.; NeurIPS / 2023-12-09. Abstract. Experiments on specified historical language models; show potential unfaithfulness of generated explanations, not that all explanations are always misleading.

[Read the source](#)

[3] SLSA v1.2: Build Provenance

SLSA project / Version 1.2; accessed 2026-10-10. Schema; buildDefinition and runDetails. Version 1.2 concerns software build provenance. The decision-lineage analogy is mayden interpretation; SLSA does not certify business legitimacy or semantic truth.

[Read the source](#)

[4] SP 800-92: Guide to Computer Security Log Management

NIST / 2006-09. Abstract. Foundational log-management guidance published in 2006; not an AI-specific standard or evidence that logging alone assures decisions.

[Read the source](#)

[5] RFC 9162: Certificate Transparency Version 2.0

IETF / 2021-12. Sections 1 and 2.1. Experimental RFC for certificate transparency, not a general decision-audit standard. Inclusion and consistency proofs do not establish correctness of logged content.

[Read the source](#)

[6] Content Credentials: C2PA Technical Specification 2.2

C2PA / Version 2.2; accessed 2026-10-10. Introduction; claims and assertions. Version 2.2 is deliberately pinned. Cryptographic provenance supports verification of signed assertions and history, not the factual truth of the content.

[Read the source](#)

[7] Datasheets for Datasets

Gebru et al.; CACM / 2021-12-01. Abstract. Dataset-documentation proposal; a completed datasheet neither establishes representativeness nor guarantees data quality or lawful use.

[Read the source](#)

[8] AI Act, Article 12: Record-keeping

European Commission AI Act Service Desk / Consolidated text as at 2026-07-27; accessed 2026-10-10. Article 12(1)-(2); scope heading. Does not impose universal logging duties on every AI application or provide case-specific legal advice.

[Read the source](#)