R-JSON

A Deterministic Evidence Schema for Regulated AI

Strategic goal: Establish proprietary IP

Why Logs Are Not Evidence

Logs are:

- non-deterministic
- incomplete
- context-free
- non-replayable

Regulated environments require **proof**, not telemetry.

The Evidence Artifact

An R-JSON artifact captures:

- pre-process state
- policy binding
- retrieval provenance
- tool intent
- execution outcome

All bound to:

- time
- identity
- policy version

Once written, it is immutable.

Core Schema Components

policy_binding

Records:

- active policy ID
- jurisdiction
- enforcement mode

- specific obligations (e.g., PII masking)

retrieval_provenance

Snapshots:

- document IDs
- classification levels
- freshness validation
- allowed sources

tool_execution

Captures:

- operation-scoped permissions
- mandatory idempotency keys
- write intent vs execution result

Deterministic Replay

Each artifact includes:

- outcome hash
- model/runtime fingerprint
- retrieval snapshot references

This allows regulators to reconstruct:

what the system saw, even if models or prompts have changed.

Regulatory Use Cases

- Fair lending disputes
- GDPR residency audits
- Incident investigations
- Supervisory reviews

R-JSON becomes the **black box recorder** for AI systems.