WoI-Lab: Compliance Snapshot ? Open for Collaboration and Research

Version: 1.0

Status: Verified Prototype

Date: 2025-11-07 18:24:34Z

1. System Description

A deterministic, traceable AI reasoning pipeline for secure data processing, designed for compliance and transparency in reasoning and classification systems.

2. Functional Summary

- Dataset Hashing: SHA-256 lineage of all inputs and outputs (OK)
- Integrity Anchoring: HMAC-SHA256 + combined cryptographic chain (OK)
- Secure Encoding/Decoding: Non-semantic deterministic encoding with trace flag (OK)
- Transient Relay: Encrypted transfer via secure gateway (OK)
- Reasoning Pipeline: Async classification + reasoning engine (OK)
- Database Logging: SQLite lineage schema with cryptographic anchors (OK)
- Vocab Determinism: Immutable vocabulary generation w/ trace record (OK)

3. Regulatory Alignment

GDPR: Art. 5, 25, 32 - Data minimization, traceable anonymization, verifiable integrity

EU AI Act: Title IV, Art. 53?56 - Proven data lineage, human-in-the-loop audit trails

FDA GMLP: Sec. IV(A)-(D) - Deterministic reproducibility, versioned reasoning audit

ISO/IEC 42001: Sec. 6.3?8.2 - Measurable AI behaviour and transparent operational logs

4. Security Layer Summary

Three-tier cryptographic approach:

- SHA-256 for all static artefacts (datasets, vocab, encoded sets)
- HMAC-SHA256 anchors for user or system identifiers (non-reversible)
- Optional encrypted relay via secure gateway (ephemeral upload, auto-delete)

5. Declaration

WoI-Lab is not a competing model.

It is a compliance framework designed to measure, secure, and validate AI behaviour - ensuring transparent and auditable operation across reasoning systems.

Open for collaboration and research.