Technical Design Note: WoI-System Architecture

Version: 1.0 — Author: Johan — WoI-Lab — Date: 2025-11-07

The WoI-Tool (Word of Information) is a modular AI measurement and reasoning pipeline designed for data integrity, interpretability, and privacy preservation. Its architecture combines cryptographic traceability with deterministic data transformation, ensuring that all encoded, decoded, and reasoning steps remain verifiable and auditable — without compromising individual or institutional data privacy.

The system is not designed to compete with large language models (LLMs), but rather to standardize, measure, and democratize their use under established ethical and regulatory frameworks.

Regulatory Alignment Summary

GDPR (EU 2016/679): Data minimization, pseudonymization, right to erasure, traceability of processing.
WoI Implementation: SHA-256 hashing of inputs; token-level pseudonymization with reversible salt encoding; separation of raw and encoded states; optional anonymized output modes.

EU AI Act (2025): Transparency, risk management, auditability, data governance, human oversight.
WoI Implementation: Deterministic manifests, reproducible encoding runs, full trace logs (.trace.json) for every transformation, operator control for reasoning modes.

FDA GMLP (Good Machine Learning Practice): Data integrity, lineage, version control, human-in-the-loop verification.
WoI Implementation: Immutable manifest system (run_manifest.json), model metadata logging, and optional operator signature verification for each run.

HIPAA (US): Privacy and integrity for health-related data.
WoI Implementation: Hash-based token obfuscation with secure key storage; no plaintext exposure beyond local or encrypted containerized runtime.

21 CFR Part 11 (Electronic Records): Authenticity, integrity, and confidentiality of digital records.
WoI Implementation: Digital signatures (HMAC-based trace keys), immutable JSONL logs, audit chain with timestamps, model identifiers, and environmental metadata.

Architectural Layers

Layer 1: Structural Integrity
Hashing of raw input and intermediate files.
Mechanism: SHA-256 checksum verification for every file, including vocab, encoded, and decoded data.

Layer 2: Semantic Obfuscation
Non-reversible token hashing with deterministic salts.
Mechanism: Ensures GDPR pseudonymization; prevents unauthorized reconstruction of sensitive text.

Layer 3: Cryptographic Validation
Master and subkey HMAC signature derivation.
Mechanism: Controlled cryptographic lineage, operator-specific traceable keys.

Layer 4: Transport / Access Encryption
Optional PHP/API layer for encrypted transmission and access control.
Mechanism: AES or bcrypt encryption; isolated Docker runtime; secure key handling and limited lifetime tokens.

Traceability & Documentation

Each process step — from CSV ingestion to reasoning output — generates a signed and timestamped trace manifest:

- run_manifest.json — dataset hash, environment info, seed, model, timestamp.
- .trace.json — per-output lineage log with source SHA-256, decoded status, and WOI_TRACE_ID.
- key_trace.json — records cryptographic key origin, entropy quality, and operator context.

This guarantees full provenance and reproducibility in line with FDA data integrity principles (“ALCOA+”).

Ethical and Societal Principles

Transparency by design – every step, every model call, every transformation is logged and inspectable.

Privacy by architecture – user data is never exposed in plaintext after ingestion.

Accountability by trace – cryptographic lineage allows trust without dependence on central authority.

Human interpretability – outputs are human-readable and measurable, not opaque model states.

Conclusion

The WoI-Tool fulfills the technical and ethical requirements demanded by modern AI regulatory frameworks — including GDPR, the EU AI Act, and FDA guidance for trustworthy AI.

Its architecture provides: End-to-end data lineage; Multi-layer encryption and key integrity; Deterministic, reproducible transformations; Full transparency, auditability, and democratic control.

This system does not compete with Large Language Models. It empowers them — enabling AI democracy, where transparency, privacy, and scientific integrity coexist within a measurable and verifiable framework.