

v3.4-SEC-005 – Zero-Knowledge Enforcement & Data Non-Retention

Document Title	Zero-Knowledge Enforcement & Data Non-Retention
Version	v3.4
Document ID	v3.4-SEC-005
Date	2025-03-22
Author	Take Back Your Data – ZK Compliance Unit
Document Type	Public / Certification / Internal

1. Purpose & Scope

This document defines the implementation and enforcement of Zero-Knowledge principles and strict data non-retention policies in MaxOneOpen. It guarantees user sovereignty, eliminates passive surveillance vectors, and ensures legal compliance under UDUH.

2. Zero-Knowledge Architecture

- All interactions are abstracted into verifiable commitments
- ZKPs used to validate state without revealing input or content
- No intermediate data is stored, transmitted or logged
- Runtime only exposes hashed execution metadata

3. Data Non-Retention Policy

Data Type	Retention Rule	Override Condition
Prompt Input	Ephemeral, destroyed post-use	None
Context Layer	Volatile unless scoped by user	Explicit session extension
Inference Result	Returned, not retained	User policy request
Audit Logs	ZKP-compatible hash only	Signed mesh fallback

4. Runtime ZK Enforcement

- ZK constraints applied at twin activation
- Tokens and identities are blinded from core logic
- Commitments are validated before output is returned
- Forks must support native or wrapped ZK proof logic

5. UDUH Alignment & Auditability

- No centralized logs or storage allowed
- All forks must document retention map
- User-triggered storage must be local, encrypted, and voluntary
- Certification requires ZK conformance test results

6. Certification Relevance

Zero-Knowledge logic and strict non-retention policies are mandatory for MaxOneOpen certification. Any fork or deployment must comply fully with cryptographic enforcement of user sovereignty.