

v3.4-DAT-001 – Sovereign Data Models & Interoperability Framework

Document Title	Sovereign Data Models & Interoperability Framework
Version	v3.4
Document ID	v3.4-DAT-001
Date	2025-03-22
Author	Take Back Your Data – Data Systems Unit
Document Type	Public / Certification / Internal

1. Purpose & Scope

This document defines the structure and enforcement of sovereign data models and interoperability protocols in MaxOneOpen. It guarantees that all data operations remain user-controlled, format-consistent, and legally independent from external providers.

2. Data Model Design

- Each data object is schema-bound and context-aware
- All fields must support typed validation and role scoping
- User control includes full schema override and encryption policies
- Supported formats: JSON+, ZK-Protobuf, Self-describing DAG

3. Interoperability Interfaces

Interface	Purpose	Sovereignty Rule
DataEx	Transfer data between twins	Only encrypted + signed payloads
VaultSync	Access local user vault	Requires ZK identity + access ticket
SchemaCast	Validate external format	Mapping must remain client-side
MetaPulse	Context sync between layers	No raw data transfer permitted

4. Federation & Compatibility Logic

- Forks must publish schema compatibility guides
- All nodes in a federated setup must enforce local validation
- Shared formats require consensus-based governance or local overrides
- No cloud-only connector may bypass sovereignty constraints

5. ZK-Compliance & Legal Independence

- Data fields must be provable without content exposure
- Interop bridges must implement ZK masking for sensitive fields
- Users can revoke schema compatibility at any time
- All data storage must be unlinkable to provider identity

6. Certification Relevance

Forks and implementations must guarantee schema transparency, sovereignty enforcement and ZK-compliant interoperability to be MaxOneOpen certified.