

## v3.4-FND-004 – Regulatory & Legal Positioning

Document Title	Regulatory & Legal Positioning
Version	v3.4
Document ID	v3.4-FND-004
Date	2025-03-22
Author	Take Back Your Data – Legal Strategy Group
Document Type	Public / Certification / Internal






### 1. Legal Purpose

This document outlines the legal and regulatory context in which MaxOneOpen operates. It ensures that self-hosted MaxOneOpen deployments are fully compliant with current and foreseeable privacy, data protection, and digital sovereignty laws.

### 2. Legal Frameworks Covered

- GDPR (EU) and ePrivacy Directive
- Digital Services Act (DSA) and Digital Markets Act (DMA)
- AI Act (EU, expected 2025)
- NIS2 Directive (cybersecurity compliance)
- ISO/IEC 27001 / 27701 (information security & privacy)

### 3. Legal Principles Embedded

-  **\*\*UDUH\*\***: ‘User Data in User Hands’ as default data flow
-  **\*\*No central data capture\*\***: All deployments are non-intrusive and decentral
-  **\*\*Verifiability\*\***: All actions are protocol-based, cryptographically logged
-  **\*\*Purpose limitation\*\***: All components are constrained to specific lawful functions
-  **\*\*Customizable policy enforcement\*\***: Templates for controller/processor roles included

### 4. Legal Differentiator vs. BigTech

Aspect	BigTech AI	Open Source LLM	MaxOneOpen
Data Sovereignty	❌ External Processing	⚠️ Optional	✅ Fully local / verifiable
GDPR Compliance	⚠️ Unclear roles	⚠️ Depends on use	✅ By design
Lawful Purpose Boundaries	❌ Vague or none	⚠️ Developer-defined	✅ Built into architecture
Controller/Processor Mapping	❌ Vendor-defined	⚠️ Manual templates	✅ Automated role assignment

## 5. Certification Relevance

This document is mandatory for any entity seeking a MaxOneOpen certification under privacy and compliance criteria. It provides the structural argumentation for how the architecture satisfies key legal requirements by design, not by disclaimer.