

# Souveräne KI-Governance auf Gemeinschaftsebene: Ein EU Policy Brief

John Stroh, Director, My Digital Sovereignty Limited

2026-04-18

## Contents

<b>Souveräne KI-Governance auf Gemeinschaftsebene</b>	<b>1</b>
Ein EU Policy Brief . . . . .	1
Zusammenfassung . . . . .	2
1 - Was wurde gebaut, und warum . . . . .	3
2 - Die drei Mechanismen . . . . .	4
2.1 Die Situierete Sprachschicht (SLL) . . . . .	4
2.2 Wächter-Agenten . . . . .	5
2.3 Föderation . . . . .	6
Nr. 3 - EU-Regulierungshaken . . . . .	7
3.1 AI-Gesetz - Artikel 2 und 50 . . . . .	7
3.2 Europäisches Gesetz zur Medienfreiheit . . . . .	7
3.3 GDPR - Artikel 9 . . . . .	8
3.4 Gesetz über digitale Dienste und CLOUD-Gesetz . . . . .	8
4 - Strukturelle Prüfungskriterien . . . . .	9
5 - Was übertragbar ist und was nicht . . . . .	10
6 - Drei Fragen, die dieser Schriftsatz nicht beantwortet . . . . .	11
7 - Gegenwärtiger Stand, Lizenzierungssituation und Fahrplan . . . . .	12
8 - Wie man sich engagiert . . . . .	13
Danksagungen und Offenlegungen . . . . .	14
Vorgeschlagene Zitate . . . . .	14

## Souveräne KI-Governance auf Gemeinschaftsebene

### Ein EU Policy Brief

**Wie Gemeinschaftsorganisationen und kleine Unternehmen die Verpflichtungen des AI Act erfüllen können, ohne die Kontrolle an ihren Verkäufer zu delegieren.**

**Autor** — John Stroh, Direktor, My Digital Sovereignty Limited, Neuseeland **ORCID** — [0009-0005-2933-7170](https://orcid.org/0009-0005-2933-7170) **DOI** — [10.5281/zenodo.19635598](https://doi.org/10.5281/zenodo.19635598) **Übergeordnetes Papier** — *Distributive Equity Through Structure: A Community-Scale Worked Example of Values*

*Stickiness* (v1.0, 2026-04-16). DOI: [10.5281/zenodo.19600614](https://doi.org/10.5281/zenodo.19600614). **Version** — 0.1 (veröffentlicht 2026-04-18) **Lizenz** — Creative Commons Namensnennung 4.0 International (CC BY 4.0) **Korrespondierender Autor** — john.stroh@mysovereignty.digital **Auch verfügbar auf** — Englisch (<https://agenticgovernance.digital/whitepapers/eu-policy-brief>)

---

## Zusammenfassung

Die meisten EU-Gemeinschaftsorganisationen werden das KI-Gesetz erfüllen, indem sie die Vorgaben ihres bestehenden Anbieters akzeptieren. Der Anbieter bestimmt das Modell, den Umgang mit den Daten und die gerichtliche Weiterleitung jeder Anfrage. Die Gemeinschaftsorganisation übernimmt all dies durch die Unterzeichnung eines Beschaffungsformulars. Das ist keine Compliance, sondern Delegation.

Eine Alternative ist bereits in Produktion. Die Village-Plattform, die auf einer dreischichtigen konstitutionellen Architektur aufbaut, die die Werte der Gemeinschaft im Code der Plattform verankert, sowie auf einem Situated Language Layer, der auf das von der Gemeinschaft autorisierte Material trainiert ist, bietet ganz oder teilweise eine Lösung für viele der Fälle, in denen die Delegation von Anbietern scheitert. Dieses Dokument beschreibt die drei Mechanismen, ordnet sie dem jeweiligen EU-Rechtsrahmen zu und beschreibt die strukturellen Prüfkriterien, die eine Gemeinschaft oder ein Unternehmen für sich selbst durchführen kann, bevor es ein Modul übernimmt.

Das Village Toolkit basiert auf einem Kontext, der nicht die EU ist. Es wurde im Rahmen von Te Tiriti o Waitangi (dem Vertrag von Waitangi aus dem Jahr 1840) entwickelt, der die Māori-Gemeinschaften in Neuseeland verpflichtet - wo die Datensouveränität eine verfassungsmäßige Verpflichtung zwischen der Krone und den iwi (Stämmen) ist und nicht eine regulatorische Präferenz. Um diesen Anforderungen gerecht zu werden, war eine Architektur erforderlich, bei der die Werte im Code und nicht in Marketingtexten verankert sind. Die gleiche Architektur entspricht den Verpflichtungen, die EU-Organisationen gemäß dem AI Act, der GDPR und der EMFA haben. Das Toolkit verfügt über drei Mechanismen:

1. **Der Situated Language Layer (SLL).** Ein auf die Gemeinschaft zugeschnittenes Sprachmodell, das auf von der Gemeinschaft autorisiertem Material trainiert wird und das Vokabular in den Sprachen von Minderheiten und der Gemeinschaft lokal souverän hält, anstatt es in einem globalen Korpus zusammenzufassen.
2. **Guardian Agents** Laufzeitüberprüfungen der Governance, die jede KI-Antwort anhand der erklärten Werte der Gemeinschaft bewerten, bevor die Antwort einen Benutzer erreicht. Die Einhaltung der Werte wird durch den Code erzwungen, nicht durch Grundsatzdokumente.
3. **Föderation.** Bilaterale Vereinbarungen zwischen souveränen Community-Plattformen, die es ihnen ermöglichen, sich zu verbinden - für Fahrgemeinschaften, gemeinschaftsübergreifende Ankündigungen, Videoanrufe - ohne Daten, Benutzeridentität oder Governance-Autorität an einen zentralen Vermittler abzugeben.

Jeder Mechanismus entspricht einer EU-Regelung: Artikel 2 und 50 des AI-Gesetzes (Anwendungsbereich und Transparenz); das Europäische Medienfreiheitsgesetz (Medienpluralismus in Minderheitensprachen); Artikel 9 der Datenschutz-Grundverordnung (besondere Datenkategorien, die sich wohl auch auf kulturelle Daten in Minderheitensprachen erstrecken). Das Tractatus Framework (die Governance-Ebene, auf der die Mechanismen basieren) ist Open Source unter Apache 2.0 und öffentlich auf Codeberg; die Codebasis der Village-Plattform ist derzeit proprietär, wobei bestimmte Module für eine Open-Source-Veröffentlichung in Erwägung gezogen werden, die dem in §7 beschriebenen Governance-Prozess unterliegt. Die Produktion läuft auf einer von der EU unabhängigen Infrastruktur (OVH France) und einer von Neuseeland unabhängigen Infrastruktur (Catalyst Cloud), ohne Abhängigkeiten von den USA im Anforderungspfad.

Die Behauptung dieses Kurzberichts ist nicht, dass EU-Minderheitensprachgemeinschaften das neuseeländische Toolkit pauschal übernehmen sollten. Die Forderung ist enger gefasst: Eine bestimmte Gemeinschaft oder ein bestimmtes Unternehmen - Walisisch, Sámi, Baskisch, Sorbisch, Friesisch, Katalanisch, Bretonisch oder jedes andere Leitungsorgan, jede nationale Mitgliedsorganisation mit lokalen Ortsverbänden, jeder Berufsverband, jeder Sportverband, jede Gemeindegruppe oder jeder Verein, jedes kleine Unternehmen, jede Genossenschaft, jedes Naturschutz- oder Ehemaligen-Netzwerk, jedes Gemeindeforum oder jede grenzüberschreitende Diaspora - könnte ein bestimmtes Modul unter einem bestimmten rechtlichen Rahmen übernehmen, der auf die eigene Gerichtsbarkeit zugeschnitten ist. Die Souveränität von Minderheitensprachen ist der Hauptfall, weil er die schärfsten Rechenschaftspflichten mit sich bringt; für die einfacheren Fälle gilt das gleiche Instrumentarium. Die Diskussion, die wir mit diesem Brief eröffnen wollen, dreht sich um *welches Modul, welche Gemeinschaft, welchen rechtlichen Rahmen*.

---

## **1 - Was wurde gebaut, und warum**

My Digital Sovereignty Ltd (Neuseeland) betreibt Village: eine auf Vorlagen basierende Plattform für die Verwaltung auf Gemeinschaftsebene. Eine einzige Codebasis passt sich über das Vokabular, die Funktionen und die Voreinstellungen für die Verwaltung an die spezifische Lebensform jeder Gemeinschaft oder Organisation innerhalb vernünftiger Grenzen an: Regierungsorgane und ihre Ausschüsse; nationale Mitgliedsorganisationen mit lokalen Ablegern (Berufsverbände, Handlungsgremien, Sportverbände, Konfessionen, Gewerkschaften, nationale Wohltätigkeitsorganisationen); Gemeinschaftsgruppen und Clubs (die Vereine, die eine so dichte Schicht des bürgerlichen Lebens in Deutschland bilden, sind eine natürliche Ergänzung); kleine Unternehmen; Genossenschaften; Naturschutz- und Alumni-Netzwerke; Gemeindeforen; Mitfahrzentralen; whānau (Māori-Großfamilien) - unter anderem. Wenn eine einzelne Gemeinschaft funktional unterschiedliche Arbeitsgruppen enthält, übernimmt die Föderation (§2.3) die Sequestrierung: jede Gruppe betreibt ihre eigene souveräne Instanz und vereinbart bilateral, was über die Instanzen hinweg geteilt werden soll. Die Vorlagenbibliothek wird erweitert, wenn neue Gemeinschaftstypen hinzukommen; es handelt sich nicht um einen festen Katalog.

Die Plattform existiert, weil zwei Faktoren zusammenkamen. Der erste ist der Druck der Souveränität: Die Māori-Gemeinschaften, die ihre Rechte gemäß Te Tiriti o Waitangi und den im Bericht des *Waitangi Tribunal WAI 262* und den *CARE Principles for Indigenous Data Governance* formulierten Grundsätzen geltend machen, verlangen, dass ihre Daten unter ihrer eigenen Autorität verbleiben, gemäß ihren eigenen Tikanga (Gewohnheitsprotokollen) verwaltet werden und auf einer Infrastruktur liegen, über die sie eine echte Kontrolle ausüben können. Der zweite ist ein technischer Druck: Der KI-Stack leitet jede Abfrage durch die Infrastruktur, die einer kleinen Anzahl von US-Unternehmen gehört, macht die Daten jeder Gemeinschaft zu einem Trainingsinput für diese Unternehmen und importiert die US-Rechtsprechung (insbesondere den CLOUD Act) in jede EU- oder neuseeländische Gemeinschaft, die das Auftragsformular unterzeichnet.

Village begegnet dem ersten Druck durch das Design und dem zweiten Druck durch die Bereitstellung. Die Plattform ist standardmäßig föderiert (jede Gemeinschaft ist ihre eigene juristische Einheit), mieterisoliert (kein gemeinschaftsübergreifender Datenzugriff möglich, auch nicht durch den Betreiber der Plattform) und führt Schlussfolgerungen auf einem Situated Language Layer aus, der auf neuseeländischem Material basiert. Der Anfragepfad enthält keine US-Unternehmen.

Produktions-Mieterinstanzen sind heute sowohl bei OVH France als auch bei Catalyst Cloud New Zealand in Betrieb und decken Leitungsgremien, Mitgliedergremien, Gemeindefnetzwerke, Ausschüsse, whānau (Māori-Großfamilien)-Gemeinschaftsseiten und andere Konfigurationen aus der Vorlagenbibliothek ab. Eine separate Sammlung von Demonstrationsinstanzen, die deutlich als solche gekennzeichnet sind, wird ebenfalls auf derselben Infrastruktur gehostet, so dass jeder Leser ein funktionierendes Beispiel für jede Konfiguration besuchen kann. Die erste föderierte Fahrgemeinschaft in einer Reihe von neuseeländischen Städten wird in Abschnitt 2.3 als praktisches Beispiel beschrieben. Der Rest dieses Dokuments beschreibt jeden Mechanismus, die EU-Verordnung, die er erfüllt, und die Prüfkriterien, die ein Anwender selbst überprüfen kann.

---

## **2 - Die drei Mechanismen**

### **2.1 Die Situierete Sprachschicht (SLL)**

Ein Situated Language Layer ist ein Sprachmodell, das auf die Gemeinschaft zugeschnitten ist. Sein Trainingskorpus ist das, was die Gemeinschaft entscheidet; seine Inferenz erfolgt auf einer Infrastruktur, die die Gemeinschaft überprüfen kann; seine Ergebnisse dienen den Definitionen der Gemeinschaft für akzeptablen Sprachgebrauch und nicht dem statistischen Durchschnitt eines globalen Korpus.

Im Village-Einsatz wird die Basis-SLL auf neuseeländischem Material trainiert - te reo Māori (die Māori-Sprache), neuseeländisches Englisch, Te Tiriti o Waitangi-Stipendium und Material der Gemeindeverwaltung, das von den Gemeinden, denen es gehört, für das Training freigegeben wurde. Darüber hinaus gibt es Spezialisierungen für die einzelnen Gemeinschaften: eine bischöfliche SLL hat andere Vorgaben für die Schrift und die Verwaltung als eine Whānau SLL, die wiederum andere Vorgaben

hat als eine SLL für eine Mitgliedsorganisation.

Der Bezug zu den EU-Minderheitensprachen ist unmittelbar. Eine walisischsprachige SLL, die für walisischsprachiges Material unter der Autorität einer walisischen Gemeinschaft geschult ist, würde walisischsprachige Anfragen aus walisischsprachigen Quellen beantworten. Eine samische SLL würde dasselbe für die Sami tun. Eine baskische SLL für Baskisch. Die Toolchain geht nicht speziell von te reo Māori aus - sie geht davon aus, dass die Gemeinschaft die Hoheit darüber hat, was das Modell trainiert und was das Modell tun darf. Wenn Sie Māori-Gemeinschaften durch walisische, sámische oder baskische Gemeinschaften ersetzen, müssen Sie nur mit einem anderen Korpus trainieren und nicht die Architektur neu aufbauen. Dasselbe Muster gilt für jede Gemeinschaftsorganisation - Kirchengemeinde, Genossenschaft, Naturschutzgruppe - deren Sprache zufällig die dominierende Landessprache ist: weniger sprachliche Zwänge, dieselbe Haltung der Souveränität.

Die technische Realität ist spezifischer als der Marketinganspruch. SLLs sind Basis-sprachmodelle, die auf dem Material der Gemeinschaft abgestimmt sind; sie werden nicht von Grund auf neu erstellt. Der Anspruch auf Souveränität besteht darin, dass die Feinabstimmung, die Steuerung der Inferenzzeit und das Hosting unter der Autorität der Gemeinschaft stehen - das ist die operative Bedeutung von "souverän" in diesem Zusammenhang. Woher das Basismodell selbst stammt, ist weniger wichtig, als in den meisten Debatten angenommen wird, vorausgesetzt, die Gemeinschaft kontrolliert, was damit gemacht wird und wo es läuft.

## 2.2 Wächter-Agenten

Guardian Agents sind in Code implementierte Laufzeitprüfungen, die jede von der KI erzeugte Antwort auswerten, bevor sie den Benutzer erreicht. Jede Prüfung liest die Antwort, vergleicht sie mit einem oder mehreren deklarierten Werten und lässt die Antwort entweder zu, markiert sie oder lehnt sie ab. Die deklarierten Werte werden von der Community verfasst; die Prüfungen sind Open Source.

Dies ist aus einem bestimmten Grund wichtig. Die Klebrigkeit der Werte ist die Frage, ob die erklärten Werte einer Plattform ihrer erklärten Form treu bleiben, wenn die Plattform wächst. Die übliche Antwort lautet, dass dies nicht der Fall ist: Plattformen schreiben ihre Werteerklärungen bei der Gründung und ändern sie im Laufe der Zeit unter dem Druck des Marktes, der Investoren oder der Behörden. Wertever-schiebung ist der Fachbegriff für diese Pathologie. Guardian Agents sind ein Versuch, die Drift zur Laufzeit erkennbar zu machen, nicht nur zum Zeitpunkt der Pressekonferenz. Eine KI-Antwort, die einen Guardian Agent mit den erklärten Werten einer Gemeinschaft durchlaufen hat, hat eine tatsächliche Prüfung bestanden, nicht nur eine Zusicherung von Richtlinien.

Die Analogie zur EU-Regulierung ist einfach: Artikel 50 des KI-Gesetzes über Transparenzpflichten verlangt, dass KI-generierte Inhalte identifizierbar sein müssen. Guardian Agents gehen noch weiter: Sie zeichnen für jede Antwort auf, welche Werte geprüft wurden und was die Prüfung ergeben hat. Dies ist ein prüfungsfähiges Artefakt, das eine Aufsichtsbehörde, ein Community Board oder ein Forscher direkt einsehen kann. Es ist die Art von Beweis, die eine Plattform, die behauptet, Werte zu besitzen, von einer Plattform unterscheidet, die nachweist, dass sie sie besitzt.

## 2.3 Föderation

Föderation im dörflichen Sinne ist die enge technische Vereinbarung, die es zwei souveränen Community-Plattformen ermöglicht, sich für bestimmte Zwecke zu verbinden - gemeinschaftsübergreifende Videoanrufe, gemeinsame Fahrgemeinschaften, gemeinsame Veranstaltungen, dorfübergreifende Ankündigungen - ohne dass eine der beiden Plattformen Daten, Identität oder Verwaltungsbefugnisse an eine dritte Partei abgeben muss. Jeder Zusammenschluss ist ein bilaterales Abkommen: Die beiden Gemeinschaften vereinbaren zu den von ihnen festgelegten Bedingungen, die jeweilige Interaktion zu ermöglichen. Kein zentrales Netzwerk koordiniert. Jede der beiden Parteien kann jederzeit aussteigen. Eine Föderation, der eine Gemeinschaft nicht beigetreten ist, ist eine Föderation, die für diese Gemeinschaft nicht existiert.

Der Gegensatz zum Plattformmodell ist der Punkt. Facebook-Gruppen, Discord-Server, WhatsApp-Communities und ihre Äquivalente sind keine Föderation; sie sind Instanzen innerhalb des Netzwerks eines Betreibers. Der Betreiber legt die Regeln fest, sieht die Daten und kann beides ändern. Die Föderation von Village hat die entgegengesetzte Architektur: Zwei souveräne Betreiber vereinbaren zu ihren eigenen Bedingungen eine begrenzte Interaktion. Wenn einer der beiden weggeht, geht auf der anderen Seite nichts kaputt.

**Ein praktisches Beispiel - im Bau** Die erste föderierte Fahrgemeinschaft mit mehreren Instanzen, die eine Reihe von neuseeländischen Städten verbindet, befindet sich im Bau und wird voraussichtlich Anfang Mai 2026 betriebsbereit sein. Jede Stadt wird ihre eigene souveräne Instanz betreiben - ihre eigenen Mitglieder, ihre eigene Moderation, ihre eigenen Daten. Die Städte vereinbaren bilateral, die Fahrtenvermittlung über ihre gemeinsamen Grenzen hinweg zu teilen, und nur das: keine Mitgliedschafts-, Zahlungs- oder Fahrtenverlaufdaten werden zwischen den Instanzen ausgetauscht; jede Stadt behält sich das Recht vor, den Verband jederzeit zu verlassen, wobei die Dienste der übrigen Städte davon unberührt bleiben. Die Infrastruktur des Verbunds, auf der dies ablaufen wird - das Modell FederationAgreement, die Routen und die Dienste - wird heute in der Codebasis der Plattform bereitgestellt; die Bereitstellung der Fahrgemeinschaft ist der erste Verbund mit mehreren Instanzen, der darauf basiert. Das Muster ist das Muster; die Tatsache, dass es sich um Fahrgemeinschaften handelt und nicht etwa um eine landesweite Mitgliedsorganisation, die die Zentrale mit ihren Sektionen verbindet, ist nebensächlich.

Dies hat eine unmittelbare regulatorische Bedeutung im Rahmen des Europäischen Medienfreiheitsgesetzes, das verlangt, dass die Sprachgemeinschaften der Minderheiten die redaktionelle und verwaltungstechnische Souveränität über die Medien und Informationsdienste behalten, über die sie agieren. Ein Föderationsmodell bewahrt diese Souveränität als architektonische Eigenschaft, nicht als politische Verpflichtung.

## Nr. 3 - EU-Regulierungshaken

In Abschnitt 2 wurde jede Verordnung als Ergebnis eines Mechanismus betrachtet; in diesem Abschnitt wird jeder Mechanismus als Antwort auf eine Verordnung betrachtet.

Die drei oben genannten Mechanismen überschneiden sich speziell mit vier EU-Rechtsinstrumenten. Jede Überschneidung ist eng gefasst; nichts in diesem Brief ist eine Behauptung über die Einhaltung von Vorschriften (der Autor ist kein Anwalt und handelt auch nicht als solcher).

### 3.1 AI-Gesetz - Artikel 2 und 50

**Artikel 2 (Anwendungsbereich).** Das KI-Gesetz gilt für Anbieter und Betreiber von KI-Systemen innerhalb der Union sowie für Anbieter außerhalb der Union, deren KI-Systeme in der Union genutzt werden. Eine EU-Gemeinschaft, die einen in den USA gehosteten kommerziellen KI-Dienst nutzt, ist ein Bereitsteller gemäß Artikel 2; der Betreiber dieses Dienstes ist ein Anbieter. Die Frage der Governance - wer entscheidet, wie das KI-System konfiguriert wird, was es tun darf und was nicht, und wer haftet, wenn es Fehler macht - wird durch die Wahl des Anbieters durch den Bereitsteller geregelt. Wenn Sie die Vorgaben des Anbieters akzeptieren, wird die Entscheidung über die Steuerung delegiert; Artikel 2 entbindet den Bereitsteller nicht von seiner Haftung.

**Artikel 50 (Transparenzpflichten).** Der Bereitsteller muss den Nutzern, die von den Ergebnissen eines KI-Systems betroffen sind, mitteilen, dass die Ergebnisse von KI generiert wurden und um welche Art von System es sich handelt. Dies führt zu einer ständigen Prüfungspflicht: Eine Gemeinschaftsorganisation, die keine Aufzeichnungen darüber vorlegen kann, was ihr KI-System tun sollte, mit welchen Werten es verglichen wurde und was es ausgegeben hat, kann die Transparenzpflicht nicht sinnvoll erfüllen. Guardian Agents erstellen genau diese Aufzeichnungen, und zwar automatisch und pro Antwort.

### 3.2 Europäisches Gesetz zur Medienfreiheit

Die EMFA (Verordnung 2024/1083, gültig ab 8. August 2025) schützt die redaktionelle Unabhängigkeit und den Medienpluralismus in der gesamten Union. In den Erwägungsgründen wird die besondere Stellung von Medien, die von Minderheiten gesprochen werden, und von Medien auf Gemeindeebene anerkannt. Es handelt sich dabei um Dienste, deren Publikum klein ist, deren kulturelle Funktion aber nicht durch größere Medien ersetzt werden kann.

Das Föderationsmodell von Village ist ein Gestaltungsmuster, das die EMFA zwar voraussetzt, aber nicht beschreibt. Zwei minderheitensprachige Gemeinschaftsplattformen, die sich zu vereinbarten Bedingungen zusammengeschlossen haben, bewahren die Pluralität, die die EMFA schützt. Eine Gemeinschaftsplattform, die von einem sozialen Netzwerk in amerikanischem Besitz abhängt, tut dies nicht: Ihre redaktionellen Entscheidungen unterliegen den Moderationsregeln des Netzwerks und der Befugnis des Netzwerks zur Vertragsänderung. Die EMFA verbietet

nicht die zweite Vereinbarung, sondern schafft ein Argument dafür, dass die erste Vereinbarung das ist, was die politischen Ziele des Gesetzes implizieren.

### **3.3 GDPR - Artikel 9**

Artikel 9 der Datenschutz-Grundverordnung behandelt bestimmte Kategorien personenbezogener Daten (Gesundheit, sexuelle Ausrichtung, politische Meinung, Rasse oder ethnische Herkunft, religiöse Überzeugung, Gewerkschaftszugehörigkeit, genetische und biometrische Daten) als besonders schutzbedürftig. Der Begriff "Rasse oder ethnische Herkunft" umfasst auch die Identität der Sprachgemeinschaft einer Minderheit - die Daten eines Sámi-Sprechers über die Verwendung seiner Sámi-Sprachgemeinschaft sind wohl Daten über seine ethnische Herkunft im Sinne von Artikel 9. Diese Lesart ist nicht gerichtlich geklärt, aber sie ist ein vertretbarer Ausgangspunkt für eine Gemeinschaft, die ihren Anspruch auf Datenhoheit verankern will.

Die Isolierung der Mieter, die von der Gemeinschaft kontrollierte Verwaltung und das souveräne Hosting des Village-Toolkits operationalisieren Artikel 9 in einer bestimmten technischen Form. Die Daten verlassen niemals die von der Gemeinschaft autorisierte Infrastruktur; die Verarbeitungsprotokolle sind von der Gemeinschaft überprüfbar; die Zustimmung wird auf Gemeinschaftsebene und nicht nur auf individueller Ebene erteilt. Die Einhaltung von Artikel 9 ist nicht das Ziel dieser Architektur, aber die Einhaltung von Artikel 9 ist das, was diese Architektur als Nebeneffekt erzeugt.

### **3.4 Gesetz über digitale Dienste und CLOUD-Gesetz**

Zwei ruhigere Überschneidungen, die es wert sind, erwähnt zu werden. Der Digital Services Act (DSA) verpflichtet sehr große Online-Plattformen zu Transparenz und Inhaltsmoderation. Eine Gemeinschaftsplattform, die auf Gemeinschaftsebene operiert, liegt unter den Schwellenwerten des DSA, aber eine Plattform, die den DSA auslöst und minderheitensprachige Gemeinschaften beherbergen möchte, ohne sie in ihr Moderationsregime einzubeziehen, würde in dem Föderationsmodell eine der wenigen technischen Möglichkeiten finden, die ihr dies ermöglichen. Auch der DSA setzt ein Designmuster voraus, das er nicht beschreibt.

Und der US CLOUD Act - das Gesetz, das den US-Behörden einen extraterritorialen Zugriff auf die Daten von Unternehmen mit Sitz in den USA weltweit ermöglicht - ist der ungenannte Gegenspieler in jeder Diskussion über digitale Souveränität in der EU. Eine Gemeinschaft, die einen US-KI-Anbieter einsetzt, importiert den CLOUD Act als uneingestandene Bedingung in ihre GDPR-Haltung. Eine Gemeinschaft, die einen souveränen KI-Anbieter nutzt, tut dies nicht. Dies ist keine Behauptung darüber, was der CLOUD Act bewirkt oder nicht bewirkt. Es ist eine Behauptung darüber, für welche vertragsrechtliche Haltung sich eine Gemeinschaft entschieden hat, absichtlich oder aus Versehen.

## 4 - Strukturelle Prüfungskriterien

Ein Grundsatzpapier, das nur behauptet, dass die Plattform seines Verfassers "Werte enthält", wäre wertlos. Im Folgenden finden Sie spezifische Prüfkriterien, die anhand öffentlicher Artefakte überprüfbar sind und die eine Plattform, die architektonische Verpflichtungen eingegangen ist, von einer Plattform unterscheiden, die Marketingaussagen gemacht hat.

1. **Mieterisolierung.** Kann ein Betreiber oder Administrator auf der Plattformebene Mieterinhalte lesen? Village bietet drei progressiv stärkere Ebenen an:
  - **Ebene 1** (gemeinsame Datenbank, Scoping pro Mandant) - jede Abfrage filtert nach der "TenantId"; Plattform-Administrator-Konten sind in der Autorisierungsschicht ausdrücklich vom Zugriff auf Inhalte ausgeschlossen. Überprüfbar in der Open-Source-Codebasis. Dies ist die Standardschicht und reicht für die meisten Community-Mieter aus.
  - **Tier 2** (dedizierte Datenbank pro Tenant) - die Daten des Tenants befinden sich in einer eigenen MongoDB-Datenbank mit eigenen Anmeldeinformationen; die Isolierung wird an der Datenbankgrenze und nicht auf der Abfragefilterschicht durchgesetzt. Wird heute über den Dienst TenantConnection-Manager implementiert. Überprüfbar durch Inspektion des Datenbankhosts, den der eigene Administrator des Mandanten kontrolliert.
  - **Tier 3** (selbstgehostet auf der eigenen Infrastruktur des Mandanten) - der Mandant führt Village auf seinen eigenen Servern aus; der Plattformbetreiber hat keinen Zugriff auf Daten oder Konfiguration. Die Architektur unterstützt diese Ebene bereits heute; die Bereitstellung von Tools und das Support-Modell stehen auf der Roadmap (siehe §7). Überprüfbar durch den Besitz der laufenden Instanz durch den Mieter.
2. **Zuständigkeit für die Infrastruktur** Wo verläuft der Anforderungspfad? Welchen Unternehmen gehört die darunter liegende Infrastruktur? Besteht im Anfragepfad eine explizite oder indirekte Abhängigkeit von den USA (einschließlich CDN, DNS, Analytik, Feedback-Systeme)? Die Produktionsinfrastruktur von Village besteht aus OVH France und Catalyst Cloud New Zealand, und es gibt keine US-Abhängigkeiten im Anforderungspfad. Diese Fakten lassen sich anhand von DNS-Einträgen, der nginx-Konfiguration und den Open-Source-Bereitstellungsskripten des Projekts überprüfen.
3. **Verfassen der Werte.** Wer hat die Werte der Plattform verfasst? Wer kann sie ändern? Ist der Änderungsverlauf öffentlich? Gibt es einen Mechanismus, mit dem die Gemeinschaft einen Wert anfechten, ändern oder ein Veto einlegen kann, den die Plattform im Namen der Gemeinschaft vertritt? Die Werte und die Verfassung des Villages sind öffentlich auf [mysovereignty.digital](https://mysovereignty.digital) veröffentlicht - die Verfassung unter [/constitution.html](#) und [/village-constitution.html](#), die Werte unter [/values.html](#) und [/platform-values.html](#), mit übersetzten Versionen auf Deutsch, Französisch, Niederländisch und te reo Māori. Jeder Leser kann sie direkt einsehen, bevor er eine Entscheidung zur Annahme trifft.
4. **Laufzeitdurchsetzung.** Werden die Werte der Plattform zur Laufzeit durchgesetzt oder nur im Marketing geltend gemacht? Für eine KI-Plattform bedeutet

dies: Durchläuft jede KI-Antwort eine Wertepfung, bevor sie einen Benutzer erreicht? Guardian Agents sind der Laufzeitmechanismus dafür; ihr Quellcode und ihre Konfiguration sind offen.

5. **Open-Source-Lizenz.** Unter welcher Lizenz wird der Code der Plattform veröffentlicht? Ist diese Lizenz von der OSI anerkannt, und kann eine Anwendergemeinschaft oder ein Unternehmen den Code eigenständig neu bereitstellen, ändern und überprüfen? Es gibt zwei verschiedene Antworten:
  - Das **Tractatus Framework** - die Maschinerie auf der Governance-Ebene, die den in §2 beschriebenen Mechanismen der Wertbeständigkeit zugrunde liegt - wird unter der **Apache License 2.0** veröffentlicht und ist auf Codeberg unter <https://codeberg.org/mysovereignty/tractatus-framework> öffentlich zugänglich. OSI-zugelassen. Jeder Leser kann den Code inspizieren, forken und prüfen.
  - Die Codebasis der **Village-Plattform** ist derzeit proprietär. Die Verpflichtung besteht darin, bestimmte Module - das Föderationsprotokoll, das Vokabularsystem, die Einsatzautomatisierung und die Betreiberdokumentation - als eigenständige Open-Source-Komponenten zu veröffentlichen, die dem in §7 beschriebenen Governance-Prozess unterliegen. Eine vollständige Freigabe des gesamten Plattform-Codes ist nicht geplant. Der Grund für diesen Vorbehalt ist die Angriffsfläche, die in §7 beschrieben wird.

Die Zielgruppe der Richtlinien muss nicht alle diese Prüfungen erneut durchführen. Aber die Kriterien existieren als Checkliste, die ein Forscher, eine Aufsichtsbehörde oder ein Community Board jeder Plattform, die digitale Souveränität beansprucht, vorlegen kann. Eine Plattform, die die Checkliste nicht bestehen kann, ist noch nicht souverän; eine Plattform, die es kann, hat zumindest die technische Schwelle für den Begriff überwunden.

---

## 5 - Was übertragbar ist und was nicht

Es lohnt sich, drei Stufen der Übertragbarkeit zu benennen, damit eine übernehmende Gemeinschaft oder ein Unternehmen weiß, was sie/es sauber übernimmt, was kontextabhängig angepasst werden muss und wie das Risiko aussieht, es falsch zu machen.

**Übertragbar.** Die drei Mechanismen - SLL, Guardian Agents, Federation - sind direkt übertragbar. Jeder ist ein technisches Muster; jeder hat eine Open-Source-Implementierung; jeder kann mit dem Material, der Verwaltung und den Föderationspartnern einer anderen Gemeinschaft erneut eingesetzt werden. Ein walisischsprachiger Einsatz würde strukturell ähnlich aussehen wie ein te reo Māori Einsatz, mit anderen Trainingsdaten, anderen Governance-Vorgaben und anderen Föderationsvereinbarungen. Dasselbe gilt für eine Kirchengemeinde, eine Fahrergemeinschaft in der Nachbarschaft, eine Genossenschaft oder eine Naturschutzgruppe, die in einer einzigen Landessprache operiert - das Muster der gemeinschaftlichen Souveränität geht über den Fall der sprachlichen Souveränität hinaus. Die Toolchain

geht nicht von Neuseeland aus.

**\*\*Die Idee**, dass kulturelle Daten mit Verpflichtungen zur Vormundschaft verbunden sind - dass die Daten einer Minderheitensprachgemeinschaft nicht einfach nur Informationen sind, die unter den vom Betreiber gewählten Rahmenbedingungen verarbeitet werden können, sondern ein taonga (Schatz), der unter dem eigenen tikanga der Gemeinschaft verwaltet werden muss - hat Analogien in den Kontexten der EU-Minderheitensprachen (das walisische Konzept von *cynefin*, das sámische Konzept von *árbediehtu*, das baskische Konzept von *auzolan*). Die Entsprechungen sind nicht identisch und werden in diesem Dokument auch nicht geglättet. Es wird lediglich darauf hingewiesen, dass das neuseeländische Instrumentarium auf der Grundlage eines Souveränitätsprinzips entwickelt wurde, das europäische Entsprechungen hat, und dass die EU-Gemeinschaften ihre eigenen kontextbezogenen Anpassungen vornehmen würden.

**Risiko.** Jeder Technologietransfer aus dem Globalen Süden / indigenen Kontext in den Globalen Norden / EU-Kontext birgt das Risiko, dass die technische Form übernommen wird, während der Rahmen der Rechenschaftspflicht zurückbleibt. Der Autor dieses Briefs gibt nicht vor, dieses Risiko zu lösen. Die Verantwortung für die Aufrechterhaltung der Rechenschaftspflicht bei jeder EU-Adoption liegt bei der Adoptionsgemeinschaft und den von ihr ausgewählten Forschern, Praktikern und Rechtsberatern.

---

## 6 - Drei Fragen, die dieser Schriftsatz nicht beantwortet

Ein so kurzer Schriftsatz kann die schwierigeren Fragen nicht lösen; er kann sie nur benennen.

1. **Wer entscheidet, welches Modul für welche Gemeinschaft gilt?** Eine sámische Gemeinschaft, die die SLL annimmt, aber nicht die Guardian Agents, würde eine Wahl treffen. Auf welcher Grundlage? Wer ist befugt, diese Entscheidung zu treffen?
2. **Ist das Village-Föderationsmodell ausreichend oder ist ein föderationsübergreifendes Protokoll (Matrix, ActivityPub oder etwas anderes) erforderlich, damit mehrere souveräne Gemeinschaften in großem Umfang interagieren können?** Die derzeitige Village-Föderation ist von vornherein bilateral angelegt; ein europaweites Föderationsnetzwerk für Minderheitensprachen würde dieses Design in einer Weise betonen, die noch nicht getestet wurde.
3. **Welcher ist der richtige europäische Finanzsponsor für eine souveräne Gemeinschaftsplattform?** Eine kommerzielle Stiftung, eine Genossenschaft, ein öffentlicher Geldgeber oder ein bestehendes EU-Infrastrukturprogramm (NGIO, NLnet, Horizon Europe)? Die Antwort ist wahrscheinlich von Land zu Land und von Gemeinschaft zu Gemeinschaft unterschiedlich.

## 7 - Gegenwärtiger Stand, Lizenzierungssituation und Fahrplan

**Gegenwärtiger Stand der Plattform.** Village ist auf einer von der EU unabhängigen Infrastruktur (OVH France) und einer von Neuseeland unabhängigen Infrastruktur (Catalyst Cloud) in Produktion, hostet Tenant-Instanzen in der Vorlagenbibliothek und bedient echten Datenverkehr. Die Verfassung und die Werte werden öffentlich auf [mysovereignty.digital](https://mysovereignty.digital) mit Übersetzungen ins Deutsche, Französische, Niederländische und Te Reo Māori veröffentlicht. Die Architektur, die Plattform und das übergeordnete Whitepaper existieren heute; sie sind keine Versprechen.

**Lizenzierungshaltung.** Zwei verschiedene Instrumente gelten für zwei verschiedene Komponenten:

- Das **Tractatus Framework** - die Maschinerie der Governance-Ebene, auf der die Mechanismen der Plattform zur Einhaltung der Werte basieren - wird unter der **Apache License 2.0** veröffentlicht und ist unter <https://codeberg.org/mysovereignty/tractatus-framework> öffentlich zugänglich. Jeder Leser kann es heute inspizieren, aufspalten und prüfen.
- Die Codebasis der **Village-Plattform** ist derzeit proprietär. Der Betreiber hat sich verpflichtet, bestimmte Module schrittweise und in Phasen zu veröffentlichen: das Föderationsprotokoll, das Vokabularsystem, die Einsatzautomatisierung und die Betreiberdokumentation - als eigenständige Komponenten, die andere Betreiber unabhängig vom Rest der Plattform übernehmen können. Welche Module unter welchen Lizenzen freigegeben werden, ist eine Entscheidung, die von einem demokratisch gewählten Vorstand und einem Beirat (in Gründung) genehmigt werden muss, und keine einseitige Verpflichtung der Gründer.
- **Eine vollständige Freigabe der Codebasis der Plattform ist derzeit nicht vorgesehen.** Die prinzipielle Einschränkung ist die Offenlegung der Angriffsfläche: Die Freigabe des vollständigen Quellcodes der Plattform würde Angreifern eine Karte der Sicherheitsarchitektur der Plattform liefern - dieselbe Sorge um die Verbreitung von Fähigkeiten, die in der veröffentlichten Mythos-Bedrohungsanalyse des Projekts für KI-Fähigkeiten im Allgemeinen zum Ausdruck kommt. Komponenten, deren Veröffentlichung zu einer solchen Aufdeckung führen würde, bleiben unter kontrolliertem Zugang, auch wenn weitere Module als Open Source veröffentlicht werden.
- Die Marke Village ist markenrechtlich geschützt; die vortrainierten Gewichte des SLL-Modells und die Trainingsdaten sind kommerzielle Güter; die Trainingsmethodik ist ein Geschäftsgeheimnis.

**Carpool - Zeitplan für ein funktionierendes Beispiel** Die erste föderierte Fahrge-meinschaft mit mehreren Instanzen in einer Reihe von neuseeländischen Städten befindet sich im Aufbau und wird voraussichtlich Anfang Mai 2026 betriebsbereit sein. Die Föderationsinfrastruktur, auf der sie laufen wird - das Modell FederationAgreement, Routen und Dienste - wird heute in der Codebasis der Plattform implementiert.

**Finanzierungslage** Zwei Anwendungen sind bei der NLnet Foundation in Arbeit: die NGI Zero Commons Fund Anwendung und die NGI Fediversity Anwendung. Der zweite Antrag ist speziell auf die Bereitstellung der Open-Source-Modulextraktion (Föderationsprotokoll, Vokabularsystem), des Toolkits für die Einsatzautomatisierung

und der Dokumentation für die Betreiber ausgerichtet, die einen unabhängigen Einsatz der Betreiber ermöglichen. Die Entscheidungen sind bei der Foundation anhängig.

**Selbst gehostete Implementierungen (Tier 3 Tenant Isolation).** Für Tenants, deren Souveränitätsanforderungen selbst das Hosting einer dedizierten Datenbank übersteigen - nationale Behörden, große Glaubensgemeinschaften, regulierte Berufsverbände, regierungsnahe Einrichtungen - unterstützt die technische Architektur heute den selbst gehosteten Betrieb, wobei der Tenant die Plattform auf der von ihm kontrollierten Infrastruktur betreibt. Das operative Paket - Automatisierung der Bereitstellung, Dokumentation für die Betreiber, Support-Modell - ist das, was mit dem Fediversity-Zuschussantrag finanziert werden soll. Solange diese Komponenten nicht vorhanden sind, ist der praktische selbst gehostete Einsatz eher eine individuelle Angelegenheit als ein unterstütztes Produkt.

**Was sicher ist und was nicht.** Die derzeitige Architektur der Plattform, die Lizenzierung von Tractatus unter Apache 2.0, die öffentliche Verfügbarkeit der Verfassung und der Werte sowie der Produktionsstatus auf souveräner Infrastruktur — all das ist sicher. Die Zeitpunkte der Modulveröffentlichungen, die Ergebnisse der Förderanträge und das Tempo der Genehmigungen durch den noch in Gründung befindlichen Vorstand und Beirat, die diese regeln, sind ungewiss. Dieser Bericht beschreibt, was heute existiert und was schriftlich zugesagt ist. Ergebnisse, die in der Entscheidungsgewalt Dritter liegen — Förderentscheidungen der NLnet Foundation, Genehmigungen durch den im Aufbau befindlichen Vorstand und Beirat — werden hier als Ungewissheiten dargestellt, nicht als zugesagte Leistungen.

---

## 8 - Wie man sich engagiert

Das übergeordnete Whitepaper - *Distributive Equity Through Structure: A Community-Scale Worked Example of Values Stickiness* (v1.0, 2026-04-16, DOI [10.5281/zenodo.19600614](https://doi.org/10.5281/zenodo.19600614)) - bietet die vollständige theoretische Grundlage für die Argumente in diesem Briefing, zusammen mit den strukturellen Prüfungskriterien in erweiterter Form, offenen Forschungsfragen in größerem Detail und einem vollständigen Zitierapparat.

Der Quellcode des **Tractatus Framework** ist öffentlich unter <https://codeberg.org/mysovereignty/framework> (Apache 2.0). Die Codebasis der **Village-Plattform** ist derzeit privat; sie wird nach und nach gemäß dem in §7 beschriebenen Plan für die Veröffentlichung von Modulen freigegeben. In der Zwischenzeit ist eine technische Überprüfung bestimmter Komponenten für institutionelle Forscher und Leser aus der Praxis auf Anfrage beim Autor erhältlich. Die Plattform ist live unter [mysovereignty.digital](https://mysovereignty.digital), mit öffentlich sichtbarer Verfassung, Werten und Demonstrationsinstanzen der Vorlagenbibliothek auf den Subdomains der Mieter, die von der Verbandsseite aus verlinkt sind.

Direkte Korrespondenz mit dem Autor: [john.stroh@mysovereignty.digital](mailto:john.stroh@mysovereignty.digital). Anfragen von Institutionen oder Politikern, Einladungen zur Mitarbeit an einer formalen politischen Analyse und Interessenbekundungen an operativen Einsätzen sind

willkommen.

Dieses Dokument wird unter CC BY 4.0 veröffentlicht. Es kann von jeder EU-Gemeinschaftsorganisation, jedem Forscher, Journalisten oder Politikanalysten unter Angabe der Quelle neu veröffentlicht, übersetzt und zitiert werden.

---

## Danksagungen und Offenlegungen

Dieses Dokument ist eine Weiterentwicklung von *Distributive Equity Through Structure* (v1.0, 2026-04-16). Der Zitierapparat des übergeordneten Papiers - der die Wissenschaft über indigene Datensouveränität (Te Mana Raraunga, die Global Indigenous Data Alliance, die CARE Principles for Indigenous Data Governance und die darin genannten Wissenschaftler) einschließt, die die architektonischen Verpflichtungen, die in diesem Briefing beschrieben werden, informiert - gilt auch hier und ist die korrekte Quelle für die Namensnennung.

Der Autor ist Geschäftsführer eines Einzelunternehmens, kein Rechtsgelehrter, kein Akademiker und kein politischer Praktiker. Die technische Arbeit wurde mit offengelegter AI-Unterstützung durchgeführt. **Keine der in diesem Dokument genannten Personen oder Organisationen hat dieses Dokument geprüft oder gebilligt.** Die Verantwortung für jede Behauptung liegt allein beim Autor.

---

## Vorgeschlagene Zitate

Stroh, J. (2026). *Sovereign AI Governance at Community Scale: An EU Policy Brief*. Version 0.1. My Digital Sovereignty Limited, Neuseeland. DOI [10.5281/zenodo.19635598](https://doi.org/10.5281/zenodo.19635598). Übergeordnetes Papier DOI [10.5281/zenodo.19600614](https://doi.org/10.5281/zenodo.19600614). Veröffentlicht unter <https://agenticgovernance.digital/whitepapers/eu-policy-brief-de>. ORCID [0009-0005-2933-7170](https://orcid.org/0009-0005-2933-7170). Lizenziert unter CC BY 4.0.

---