Sovereign AI Governance at Community Scale: An EU Policy Brief

John Stroh, Director, My Digital Sovereignty Limited

2026-04-18

Contents

Sovereign AI Governance at Community Scale **1**
An EU Policy Brief . . . 1
Executive summary . . . 2
1 — What was built, and why . . . 3
2 — The three mechanisms . . . 4
2.1 The Situated Language Layer (SLL) . . . 4
2.2 Guardian Agents . . . 4
2.3 Federation . . . 5
3 — EU regulatory hooks . . . 6
3.1 AI Act — Articles 2 and 50 . . . 6
3.2 European Media Freedom Act . . . 6
3.3 GDPR — Article 9 . . . 7
3.4 Digital Services Act and CLOUD Act . . . 7
4 — Structural audit criteria . . . 7
5 — What is, and is not, transferable . . . 9
6 — Three questions this brief does not answer . . . 9
7 — Present state, licensing posture, and roadmap . . . 10
8 — How to engage . . . 11
Acknowledgements and disclosures . . . 12
Suggested citation . . . 12

Sovereign AI Governance at Community Scale

An EU Policy Brief

How community organisations and small businesses can meet AI Act obligations without delegating control to their vendor.

Author — John Stroh, Director, My Digital Sovereignty Limited, New Zealand **ORCID** — 0009-0005-2933-7170 **DOI** — 10.5281/zenodo.19635598 **Parent paper** — *Distributive Equity Through Structure: A Community-Scale Worked Example of Values Stickiness* (v1.0, 2026-04-16). DOI: 10.5281/zenodo.19600614. **Version** — 0.1 (published 2026-04-18)

 Corresponding author — john.stroh@mysovereignty.digital **Also available in** — German (https://agenticgovernance.digital/whitepapers/eu-policy-brief-de)

Executive summary

Most EU community organisations will meet the AI Act by accepting their existing vendor's defaults. The vendor determines the model, the data-handling posture, and the jurisdictional routing of every query. The community organisation inherits all of this by signing a procurement form. This is not compliance; it is delegation.

An alternative is already in production. The Village platform — built around a three-layer constitutional architecture that anchors community values in the platform's code, and a Situated Language Layer trained on the community's own authorised material — offers, in whole or in part, a solution to many of the cases where vendor delegation fails. This brief sets out the three mechanisms, maps each to the EU regulatory hook it engages, and describes the structural audit criteria an adopting community or business can run for itself before taking any module on.

The Village toolkit is grounded in a context that is not the EU. It was built under Te Tiriti o Waitangi (the 1840 Treaty of Waitangi) obligations to Māori communities in New Zealand — where data sovereignty is a constitutional commitment between the Crown and iwi (tribes), not a regulatory preference. Meeting that constraint required an architecture where values are anchored in code, not in marketing copy; the same architecture answers the obligations EU organisations face under the AI Act, GDPR, and the EMFA. The toolkit has three mechanisms:

1. **The Situated Language Layer (SLL).** A community-scoped language model, trained on material the community authorises, that keeps minority-language and community-governance vocabulary locally sovereign rather than averaging it into a global corpus.
2. **Guardian Agents.** Runtime governance checks that evaluate every AI response against the community's declared values before the response reaches a user. Values stickiness enforced by code, not by policy documents.
3. **Federation.** Bilateral agreements between sovereign community platforms that let them connect — for carpools, cross-community announcements, video calls — without either surrendering data, user identity, or governance authority to a central intermediary.

Each mechanism maps to an EU regulatory hook: AI Act Articles 2 and 50 (scope and transparency); the European Media Freedom Act (minority-language media pluralism); GDPR Article 9 (special categories of data, which arguably extends to minority-language cultural data). The Tractatus Framework (the governance layer the mechanisms sit on) is open source under Apache 2.0 and public on Codeberg; the Village platform codebase is currently proprietary, with specific modules under contemplation for open-source release subject to the governance process described in §7. Production runs on EU-sovereign infrastructure (OVH France) and New Zealand-sovereign infrastructure (Catalyst Cloud), with no US dependencies in the request path.

The claim of this brief is not that EU minority-language communities should adopt the

New Zealand toolkit wholesale. The claim is narrower: a specific community or business — Welsh, Sámi, Basque, Sorbian, Frisian, Catalan, Breton, or for that matter any governance body, nationally-affiliated membership organisation with local chapters, professional association, sporting federation, community group or club, small business, cooperative, conservation or alumni network, parish network, or cross-border diaspora — could adopt a specific module, under a specific legal framework suited to its own jurisdiction. Minority-language sovereignty is the lead case because it carries the sharpest accountability obligations; the same toolkit answers the easier cases. The conversation this brief seeks to open is about *which module, which community, which legal framework*.

---

1 — What was built, and why

My Digital Sovereignty Ltd (New Zealand) operates Village: a template-based platform for community-scale governance. A single codebase adapts — via vocabulary, features, and governance defaults — to the specific form of life of any community or organisation within reasonable bounds: governance bodies and their committees; nationally-affiliated membership organisations with local chapters (professional associations, trade bodies, sporting federations, denominations, trade unions, national charities); community groups and clubs (the Vereine that form such a dense layer of German civic life are a natural fit); small businesses; cooperatives; conservation and alumni networks; parish networks; carpool services; whānau (Māori extended-family) community sites — among others. Where a single community contains functionally different work groups, federation (§2.3) handles sequestration: each group operates its own sovereign instance and agrees bilaterally on what to share across instances. The template library expands as new community types engage; it is not a fixed catalogue.

The platform exists because two pressures converged. The first is a sovereignty pressure: Māori communities, asserting rights under Te Tiriti o Waitangi and the principles articulated in the *Waitangi Tribunal WAI 262 report* and the *CARE Principles for Indigenous Data Governance*, require that their data remain under their own authority, governed according to their own tikanga (customary protocols), on infrastructure over which they can exercise genuine oversight. The second is a technical pressure: the commodity AI stack routes every query through infrastructure owned by a small number of US corporations, makes every community's data a training input for those corporations, and imports US jurisdiction (particularly the CLOUD Act) into every EU or New Zealand community that signs the procurement form.

Village answers the first pressure by design and the second pressure by deployment. The platform is federated by default (each community is its own jurisdictional entity), tenant-isolated (no cross-community data access is possible, including by the platform operator), and runs inference on a Situated Language Layer trained on New Zealand-grounded material. No US companies are in the request path.

Production tenant instances are live today on both OVH France and Catalyst Cloud New Zealand, covering governance bodies, membership bodies, parish networks, committees, whānau (Māori extended-family) community sites, and other configurations from the template library. A separate collection of demonstration instances, visibly

labelled as such, is also hosted on the same infrastructure so any reader can visit a worked example of each configuration. The first federated carpool across a set of New Zealand towns is described as a worked example in §2.3. The rest of this brief describes each mechanism, the EU regulation it answers, and the audit criteria an adopter can check for themselves.

---

2 — The three mechanisms

2.1 The Situated Language Layer (SLL)

A Situated Language Layer is a community-scoped language model. Its training corpus is what the community decides; its inference happens on infrastructure the community can audit; its outputs serve the community's definitions of acceptable language use rather than a global corpus's statistical average.

In the Village deployment, the base SLL is trained on New Zealand-grounded material — te reo Māori (the Māori language) vocabulary, New Zealand English, Te Tiriti o Waitangi scholarship, and community-governance material authorised for training by the communities that own it. Per-community specialisations layer on top: an Episcopal SLL has different scriptural and governance defaults than a Whānau SLL, which has different defaults than a Membership-Organisation SLL.

The relevance to EU minority languages is direct. A Welsh-language SLL, trained on Welsh-language material under a Welsh community's authority, would answer Welsh-language queries from Welsh-language sources. A Sámi SLL would do the same for Sámi. A Basque SLL for Basque. The toolchain does not assume te reo Māori specifically — it assumes that the community holds sovereignty over what trains the model and what the model is permitted to do. Substituting Māori communities for Welsh, Sámi, or Basque communities is a matter of re-training on a different corpus, not rebuilding the architecture. The same pattern applies to any community organisation — parish, cooperative, conservation group — whose language happens to be the dominant national one: fewer linguistic constraints, the same sovereignty posture.

The engineering reality is more specific than the marketing claim. SLLs are base language models fine-tuned on community material; they are not rebuilt from scratch. The sovereignty claim is that the fine-tuning, the inference-time steering, and the hosting are all under community authority — which is the operational meaning of "sovereign" in this context. Where the base model itself comes from matters less than most debates assume, provided the community controls what is done to it and where it runs.

2.2 Guardian Agents

Guardian Agents are runtime checks, implemented in code, that evaluate every AI-generated response before it reaches a user. Each check reads the response, assesses it against one or more declared values, and either passes, flags, or rejects the response. The declared values are authored by the community; the checks are open source.

This matters for a specific reason. Values stickiness is the question of whether a platform's declared values remain true to their declared form as the platform grows. The usual answer is that they do not: platforms write values statements at founding and mutate them under market, investor, or regulatory pressure over time. Values drift is the technical term for this pathology. Guardian Agents are an attempt to make drift detectable at runtime, not only at press-conference time. An AI response that has passed through a Guardian Agent with a community's stated values has passed an actual check, not a policy-statement assurance.

The EU regulatory analogue is straightforward: AI Act Article 50 on transparency duties asks that AI-generated content be identifiable. Guardian Agents go further — they record, per-response, which values were checked and what the check returned. This is an audit-ready artifact that a regulator, a community board, or a researcher can inspect directly. It is the kind of evidence that distinguishes a platform claiming to hold values from a platform demonstrating that it holds them.

2.3 Federation

Federation, in the Village sense, is the narrow technical arrangement that lets two sovereign community platforms connect for specific purposes — cross-community video calls, shared carpools, joint events, cross-village announcements — without requiring either to surrender data, identity, or governance authority to a third party. Each federation is a bilateral agreement: the two communities agree, on the terms they specify, to enable the specific interaction. No central network coordinates. Either party can exit at any time. A federation that a community has not entered is a federation that does not exist for that community.

The contrast with the platform model is the point. Facebook Groups, Discord Servers, WhatsApp Communities, and their equivalents do not federate; they are instances inside one operator's network. The operator sets the rules, sees the data, and can change both. Village's federation is opposite in architecture: two sovereign operators agree, on their own terms, to a bounded interaction. When either walks away, nothing breaks on the other side.

A worked example — in build. The first multi-instance federated carpool, connecting a set of New Zealand towns, is in build and expected to be operational in early May 2026. Each town will operate its own sovereign instance — its own members, its own moderation, its own data. The towns agree bilaterally to share ride-matching across their common boundary, and only that: no membership, payment, or trip-history data crosses between instances; each town retains the right to exit the federation at any time, after which the remaining towns' services are unaffected. The federation infrastructure this will run on — the `FederationAgreement` model, routes, and services — is deployed in the platform codebase today; the carpool deployment is the first multi-instance federation under it. The pattern is the pattern; the fact that it is carpools rather than, say, a nationally-affiliated membership body connecting HQ to its chapters, is incidental.

This has direct regulatory relevance under the European Media Freedom Act, which asks that minority-language communities retain editorial and governance sovereignty

over the media and information services through which they act. A federation model preserves that sovereignty as an architectural property, not a policy commitment.

---

3 — EU regulatory hooks

Section 2 approached each regulation as an outcome of a mechanism; this section approaches each mechanism as an answer to a regulation.

The three mechanisms above intersect specifically with four EU regulatory instruments. Each intersection is stated narrowly; nothing in this brief is a claim of regulatory compliance opinion (the author is not a lawyer and does not act as one).

3.1 AI Act — Articles 2 and 50

Article 2 (scope). The AI Act applies to providers and deployers of AI systems within the Union, and to providers outside the Union whose AI systems' output is used in the Union. An EU community using a US-hosted commercial AI service is a deployer under Article 2; the operator of that service is a provider. The governance question — who decides how the AI system is configured, what it may and may not do, and who is liable when it errs — is allocated by the deployer's choice of provider. Accepting vendor defaults delegates the governance decision; Article 2 does not relieve the deployer of the liability.

Article 50 (transparency duties). Deployers must disclose, to users affected by an AI system's output, that the output was AI-generated and the nature of the system. This creates a standing audit demand: a community organisation that cannot produce a record of what its AI system was instructed to do, what values it was checked against, and what its output was, cannot meaningfully satisfy the transparency duty. Guardian Agents produce exactly this record, automatically, per-response.

3.2 European Media Freedom Act

The EMFA (Regulation 2024/1083, applying from 8 August 2025) protects editorial independence and media pluralism across the Union. Its recitals acknowledge the special position of minority-language media and community-scale media — services whose audiences are small but whose cultural function is not substitutable by larger-scale media.

Village's federation model is a design pattern the EMFA presupposes but does not describe. Two minority-language community platforms, federated on agreed terms, preserve the plurality the EMFA protects. A community platform dependent on a US-owned social network does not: its editorial decisions are subject to the network's moderation rules and the network's contractual-change authority. The EMFA does not prohibit the second arrangement; it creates an argument that the first arrangement is what the Act's policy goals imply.

3.3 GDPR — Article 9

Article 9 of the GDPR treats certain categories of personal data (health, sexual orientation, political opinion, racial or ethnic origin, religious belief, trade union membership, genetic and biometric data) as requiring enhanced protection. The scope of "racial or ethnic origin" plausibly includes minority-language community identity — a Sámi speaker's data about their Sámi-language community use is arguably data about their ethnic origin in the Article 9 sense. This reading is not judicially settled, but it is a defensible starting point for a community seeking to anchor its data-sovereignty claim.

The Village toolkit's tenant isolation, community-controlled governance, and sovereign hosting operationalise Article 9 in a specific technical form. The data never leaves the community's authorised infrastructure; the processing record is community-auditable; consent is exercised at the community level, not just the individual level. Article 9 compliance is not what this architecture is for, but Article 9 compliance is what this architecture produces as a side effect.

3.4 Digital Services Act and CLOUD Act

Two quieter intersections worth naming. The Digital Services Act (DSA) creates transparency and content-moderation duties on very large online platforms. A community platform operating at community scale is below the DSA's thresholds; but a DSA-triggering platform that wanted to host minority-language communities without absorbing them into its moderation regime would find the federation model one of the few technical arrangements that would let it do so. The DSA, too, presupposes a design pattern it does not describe.

And the US CLOUD Act — the statute that gives US authorities extraterritorial access to data held by US-headquartered companies worldwide — is the unnamed opposing force in every EU digital sovereignty conversation. A community using a US AI provider imports the CLOUD Act into its GDPR posture as an unacknowledged condition. A community using a sovereign AI deployment does not. This is not a claim about what the CLOUD Act does or does not achieve; it is a claim about which contractual-jurisdictional posture a community has chosen, intentionally or by default.

---

4 — Structural audit criteria

A policy brief that claimed only that its author's platform "holds values" would be worthless. What follows are specific audit criteria, verifiable from public artifacts, that distinguish a platform that has made architectural commitments from a platform that has made marketing claims.

1. **Tenant isolation.** Can an operator or administrator at the platform level read tenant content? Village offers three progressively stronger tiers:
    - **Tier 1** (shared database, per-tenant scoping) — every query filters on `tenantId`; platform-admin accounts are explicitly barred from content access in

the authorisation layer. Verifiable in the open-source codebase. This is the default tier and is sufficient for most community-scale tenants.
- **Tier 2** (dedicated database per tenant) — the tenant's data lives in its own MongoDB database with its own connection credentials; isolation is enforced at the database boundary rather than the query-filter layer. Implemented today via the `TenantConnectionManager` service. Verifiable by inspecting the database host the tenant's own administrator controls.
- **Tier 3** (self-hosted on the tenant's own infrastructure) — the tenant runs Village on its own servers; the platform operator has no access to data or configuration. The architecture supports this tier today; the deployment tooling and support model are on the roadmap (see §7). Verifiable by the tenant's possession of the running instance.

2. **Infrastructure jurisdiction.** Where does the request path run? What companies own the infrastructure under it? Is there any US dependency in the request path, explicit or indirect (including CDN, DNS, analytics, feedback systems)? Village's production infrastructure is OVH France and Catalyst Cloud New Zealand, with no US dependencies in the request path. These facts are verifiable from DNS records, nginx configuration, and the project's open-source deployment scripts.

3. **Values authoring.** Who wrote the platform's values? Who can change them? Is the change history public? Is there a mechanism by which the community can contest, amend, or veto a value the platform asserts on the community's behalf? Village's values and constitution are published publicly on `mysovereignty.digital` — the constitution at `/constitution.html` and `/village-constitution.html`, the values at `/values.html` and `/platform-values.html`, with translated versions in German, French, Dutch, and te reo Māori. Any reader can inspect them directly before making any adoption decision.

4. **Runtime enforcement.** Are the platform's values enforced at runtime, or only asserted in marketing? For an AI platform, this means: does every AI response pass through a values check before it reaches a user? Guardian Agents are the runtime mechanism for this; their source code and configuration are open.

5. **Open-source licence.** Under what licence is the platform's code published? Is that licence OSI-approved, and can an adopting community or business re-deploy, modify, and audit the code independently? Two different answers apply:

   - The **Tractatus Framework** — the governance-layer machinery that underpins the values-stickiness mechanisms described in §2 — is released under **Apache License 2.0** and is public on Codeberg at `https://codeberg.org/mysovereignty/tractatus-framework`. OSI-approved. Any reader can inspect, fork, and audit.
   - The **Village platform codebase** is currently proprietary. The commitment is to release specific modules — the federation protocol, the vocabulary system, the deployment automation, and the operator documentation — as standalone open-source components, subject to the governance process described in §7. Full open-sourcing of the whole platform codebase is not planned. The driver for that reservation is attack-surface exposure, described in §7.

A policy audience does not need to re-perform all of these audits. But the criteria exist as a checklist a researcher, a regulator, or a community board can run against any platform claiming digital sovereignty. A platform that cannot pass the checklist is not yet sovereign; a platform that can has at least cleared the technical threshold for the term.

---

5 — What is, and is not, transferable

Three levels of transferability are worth naming, so that an adopting community or business knows what it inherits cleanly, what requires contextual adaptation, and what the risk of getting it wrong looks like.

Transferable. The three mechanisms — SLL, Guardian Agents, Federation — are directly transferable. Each is a technical pattern; each has an open-source implementation; each can be re-deployed with a different community's material, governance, and federation partners. A Welsh-language deployment would look structurally similar to a te reo Māori deployment, with different training data, different governance defaults, and different federation agreements. The same is true of a parish, a neighbourhood carpool, a cooperative, or a conservation group operating in a single national language — the community-sovereignty pattern generalises beyond the linguistic-sovereignty case. The toolchain does not assume New Zealand.

Requires contextual adaptation. The *idea* that cultural data carries obligations of guardianship — that a minority-language community's data is not simply information to be processed under whatever framework the operator chooses, but a taonga (treasure) to be stewarded under the community's own tikanga — has analogues in EU minority-language contexts (the Welsh concept of *cynefin*, the Sámi concept of *árbediehtu*, the Basque concept of *auzolan*). The analogues are not identical, and this brief does not flatten them. It observes only that the New Zealand toolkit was designed under a sovereignty principle that has European counterparts, and that EU communities would make their own contextual adaptations.

Risk. Any transfer of technology from a Global South / indigenous context into a Global North / EU context carries the risk of extracting the technical form while leaving the accountability framework behind. This brief's author does not pretend to resolve that risk. The responsibility for maintaining accountability in any EU adoption rests with the adopting community and its chosen researchers, practitioners, and legal advisors.

---

6 — Three questions this brief does not answer

A brief this short cannot resolve the harder questions; it can only name them.

1. **Who chooses which module applies to which community?** A Sámi community adopting the SLL, but not Guardian Agents, would be making a choice. On what basis? Who is authorised to make it?

2. **Is the Village federation model enough, or is a cross-federation protocol (Matrix, ActivityPub, something else) required for multiple sovereign communities to interoperate at scale?** The current Village federation is bilateral by design; a Europe-wide minority-language federation network would stress that design in ways that are not yet tested.
3. **What is the correct European fiscal sponsor for a sovereign community platform?** A commercial foundation, a cooperative, a public-sector grantmaker, or an existing EU infrastructure programme (NGI0, NLnet, Horizon Europe)? The answer probably differs per jurisdiction and per community.

---

7 — Present state, licensing posture, and roadmap

Present state of the platform. Village is in production on EU-sovereign infrastructure (OVH France) and New Zealand-sovereign infrastructure (Catalyst Cloud), hosting tenant instances across the template library and serving real traffic. The constitution and values are published publicly on `mysovereignty.digital` with translations into German, French, Dutch, and te reo Māori. Architecture, platform, and parent whitepaper are in existence today; they are not promises.

Licensing posture. Two different instruments apply to two different components:

- The **Tractatus Framework** — the governance-layer machinery on which the platform's values-stickiness mechanisms sit — is released under **Apache License 2.0** and is public at `https://codeberg.org/mysovereignty/tractatus-framework`. Any reader can inspect, fork, and audit it today.
- The **Village platform codebase** is currently proprietary. The operator's commitment is to open-source specific modules progressively, and in phases: the federation protocol, the vocabulary system, the deployment automation, and the operator documentation — as standalone components that other operators can adopt independently of the rest of the platform. Which modules are released under which licences is a decision subject to approval by a democratically-elected Board and Advisory Committee (in formation), not a unilateral founder commitment.
- **Full open-sourcing of the platform codebase is not presently contemplated.** The principled constraint is attack-surface exposure: releasing the full platform source would provide adversaries with a map of the platform's security architecture — the same capability-proliferation concern the project's published Mythos threat analysis articulates for AI capabilities generally. Components whose publication would create such exposure will remain under controlled access, even as more modules are open-sourced.
- The Village brand is protected by trademark; the pre-trained SLL model weights and the training data are commercial assets; the training methodology is a trade secret.

Carpool — worked example timeline. The first multi-instance federated carpool across a set of New Zealand towns is in build and expected to be operational in early May 2026. The federation infrastructure it will run on — the `FederationAgreement`

model, routes, and services — is deployed in the platform codebase today.

Funding posture. Two applications are in flight with the NLnet Foundation: the NGI Zero Commons Fund application and the NGI Fediversity application. The second of these is specifically scoped to deliver the open-source module extraction (federation protocol, vocabulary system), the deployment automation toolkit, and the operator documentation that make independent operator deployments possible. Decisions are pending with the Foundation.

Self-hosted deployments (Tier 3 tenant isolation). For tenants whose sovereignty requirements exceed even dedicated-database hosting — national agencies, large denominations, regulated professional bodies, government-adjacent entities — the technical architecture supports self-hosted operation today, with the tenant running the platform on infrastructure it controls. The operational packaging — deployment automation, operator documentation, support model — is what the Fediversity grant application is designed to fund. Until those pieces are in place, practical self-hosted deployment is a bespoke engagement rather than a supported product.

What is certain and what isn't. The platform's present architecture, licensing of Tractatus under Apache 2.0, public availability of the constitution and values, and production status on sovereign infrastructure — these are certain. Timings of module releases, grant outcomes, and the pace of the Board-and-Advisory-Committee approvals that govern them — these are uncertain. This brief describes what exists today and what is committed in writing. Outcomes that belong to third parties — grant decisions by the NLnet Foundation, approvals by the Board and Advisory Committee in formation — are described as uncertainties, not promised as deliverables.

---

8 — How to engage

The parent whitepaper — *Distributive Equity Through Structure: A Community-Scale Worked Example of Values Stickiness* (v1.0, 2026-04-16, DOI 10.5281/zenodo.19600614) — provides the full theoretical basis for the arguments in this brief, along with the structural audit criteria in extended form, open research questions in greater detail, and a full citation apparatus.

The **Tractatus Framework** source is public at `https://codeberg.org/mysovereignty/tractatus-framework` (Apache 2.0). The **Village platform codebase** is currently private; it will be released progressively per the module-release roadmap described in §7. In the interim, technical review of specific components is available to institutional researchers and policy-practitioner readers on request to the author. The platform is live at `mysovereignty.digital`, with publicly visible constitution, values, and template-library demonstration instances at the tenant subdomains linked from its federation page.

Direct correspondence to the author: `john.stroh@mysovereignty.digital`. Institutional or policy-practitioner queries, invitations to contribute to formal policy analysis, and expressions of interest in operational deployments are all welcome.

by any EU community organisation, researcher, journalist, or policy analyst with attribution.

Acknowledgements and disclosures

This brief is derived from *Distributive Equity Through Structure* (v1.0, 2026-04-16). The parent paper's citation apparatus — which includes the indigenous data sovereignty scholarship (Te Mana Raraunga, the Global Indigenous Data Alliance, the CARE Principles for Indigenous Data Governance, and the individual scholars it names) that informs the architectural commitments this brief describes — applies here as well and is the correct source for attribution.

The author is a single-founder company director, not a legal scholar, not an academic, not a policy practitioner. Technical work has been done with disclosed AI assistance. **No person or organisation named in this brief has reviewed or endorsed it.** Responsibility for every claim is the author's alone.

Suggested citation

Stroh, J. (2026). *Sovereign AI Governance at Community Scale: An EU Policy Brief*. Version 0.1. My Digital Sovereignty Limited, New Zealand. DOI 10.5281/zenodo.19635598. Parent paper DOI 10.5281/zenodo.19600614. Published at https://agenticgovernance.digital/whitepapers/eu-policy-brief. ORCID 0009-0005-2933-7170. Licensed under CC BY 4.0.