Policy Brief:
Aiming for AI Interoperability

ceimia

with support from
Google.org

1. Background

The *Aiming for AI Interoperability* report investigates the ongoing challenge of achieving regulatory and technical AI interoperability as national and global AI governance efforts are proliferating. Here, technical interoperability is the ability of AI systems and networks to function together, and regulatory interoperability is the consistency and overlap of rules across jurisdictions and sectors. This report observes an accelerating trend that many governments, standard-setting bodies, and private firms are drafting, implementing, or passing new AI laws, policies, and frameworks at a staggering pace, resulting in fragmentation and confusion for both private and public sector actors. The global AI governance landscape is beset by fragmentation along several axes: jurisdictional, sectoral, and technical. National and subnational governments – including major AI developers like the US, EU, China, and Canada – are advancing new legislative and regulatory approaches, while international organizations and standards bodies (ISO, IEEE, OECD, UN) are also producing their own standards, certifications, codes of conduct, and principles. The sheer rapidity of these parallel efforts is resulting in an increasingly convoluted and fragmented landscape which poses four broad challenges:

- Uncertainty for firms and public institutions on which standards or regulatory frameworks to comply with, especially those operating transnationally

- High barriers to entry for SME innovators and challenges for multinational organizations to scale AI deployment globally

- Potential for regulatory venue shopping and for larger firms to entrench dominance through custom-built compliance infrastructures

- The risk that technical and regulatory standards – through delayed or conflicting implementation – may become irreconcilable, requiring costly future retrofitting or even hindering trade and collaboration

Addressing these fragmentation challenges requires a multisectoral coherent strategy for regulatory and technical AI interoperability. This strategy should aim to blend early definitional standards, adaptive governance frameworks, robust verification mechanisms, and cross-sectoral collaboration. Other sectors have experienced similar challenges and aimed for interoperability – with varying degrees of success.

2. Case Studies

To identify practical pathways that can be taken to achieve AI interoperability, this report provides four sectoral case studies – each tracing their evolution of interoperability efforts.

Nanotechnology's NanoDefine Project: Before intervention, nanomaterial classification in the EU was marked by fragmented measurement protocols and a lack of standard definitions. The *NanoDefine* project was established to create consensus, validated methods, and practical tools that would enable regulatory bodies, manufacturers, and research labs to uniformly classify and measure nanomaterials. Through collaborative project management, standardized operating procedures, and a *NanoDefiner e-tool*, *NanoDefine* fostered harmonization, improved regulatory clarity, and scaled technical solutions across the EU and beyond. This proactive, adaptive approach served as a model for balancing standardization with flexibility.

Environmental Sustainability's INSPIRE Directive: The *INSPIRE Directive* sought to harmonize environmental data infrastructure among fragmented EU member states. Prior to INSPIRE, cross-border environmental policymaking was hindered by incompatible data and legacy systems. This Directive provided a phased legal mandate for standardized spatial data (like river basin management), complemented by capacity-building support for less-resourced states (like government grants). While *INSPIRE* enabled greater cross-border analytical capacity and data access, technical rigidity and uneven implementation persisted, highlighting the need for adaptive regulatory frameworks and continuous stakeholder engagement.

Telecommunication's Telegraph to Snowden and "Zero-Trust" Paradigm: Telecommunications interoperability was shaped by cycles of voluntary standardization, security crises, and evolving geopolitical priorities. The 1865 *International Telegraph Convention* set early groundwork through consensus-based protocols, but 20th-century security crises (WWI cable-cutting and post-Snowden privacy concerns) demonstrated the vulnerability of trust-based systems without verification. The shift to "zero-trust architectures" now dominates contemporary practice, emphasizing ongoing authentication, verification, and legal standards. Trust must be continually built and reinforced by technical and legal mechanisms, not assumed as a static condition.

Internet/Web Architecture's HTTP, IP, and the Rise of the "Splinternet": The open, bottom-up consensus model that drove TCP/IP's adoption enabled

considerable innovation and interoperability – largely sparked by clear US government procurement incentives. However, subsequent fragmentation – accelerated by digital sovereignty policies, content filtering, and diverging national priorities – has led to the "splinternet," where regulatory and technical interoperability are again in question. Lessons here stress the necessity of maintaining adaptive governance, multilayered technical frameworks, and ongoing stakeholder participation amidst shifting political and market forces.

3. Policy Recommendations through Sectoral Roadmaps

Using these cases, the report provides policy recommendations through sectoral roadmaps, with each roadmap tailored to that sector's unique positions in the AI landscape. The sectors are standard-setting and international organizations; NGO/civil society; public; and private sectors.

Standards-Setting and International Organizations

- Accelerate the development of crosswalks between national and international standards and frameworks, shorten development cycles for emerging standards, and support and advocate for international standards to be incorporated by reference in (sub)national regulatory efforts

- Develop international standards in a way that allows for those standards to be adopted and adapted at the local-level, allowing these standards to be sovereignty-compatible. Ensure meaningful participation of SMEs, Indigenous groups, and the Global Majority in standard-setting efforts

- International organizations should endorse existing independent and widely recognized frameworks to stabilize cooperation, reduce compliance duplication, and accelerate coherence during geopolitical disruptions

NGOs and Civil Society

- Actively stake claims to influence the scope and focus of AI technical and regulatory standards. Ensure meaningful engagement in standard-setting and technical interoperability discussions, offering expertise on protocols, security, privacy, and ethical implications

- Secure steady funding and maintain expert capacity to weather shifts in the political and philanthropic environment, while sustaining pressure for privacy, competition, and security benchmarks within policy debates

- Insist on transparent, open standards for technical protocols and raise concerns about emergent risks. This role is especially vital for ensuring checks and balances in system-wide adoption of new AI frameworks

Public Sector

- Governments should rapidly convene expert groups to set foundational definitions and measurement protocols for AI systems, prioritizing harmonization with global frameworks like the OECD's *AI Principles* and relevant ISO/IEC and IEEE standards

- Laws and regulations must be designed for iterative updating (which can be achieved through incorporation by reference), with dedicated teams for interoperability coordination and "regulatory sandboxes" to test AI systems in controlled and adaptable environments

- Invest in comprehensive auditing and mutual recognition agreements, enabling AI audit results or certifications to be portable across jurisdictions while supporting independent third-party review mechanisms

- Use government procurement power to incentivize interoperability compliance among AI vendors. Establish permanent coordination bodies modeled after Internet Engineering Task Force multistakeholder structures and prioritize cross-border partnerships, especially in critical sectors such as health, finance, transportation, and defense

Private Sector

- Conduct internal interoperability assessments, identify existing technical debt and lock-in risks, and assemble cross-functional teams to steward organizational AI governance

- Invest in technical infrastructures that use standardized APIs, interoperable data formats, and modular architectures with built-in regulatory adaptation capacities

- Implement interoperability pilot projects to test technical, compliance, and user impact in controlled settings and share best practices and results with regulators

- Establish continuous monitoring of interoperability performance and formal processes for evaluating and adopting new standards

4. Conclusion

Policymakers and decision-makers face a critical choice. They can allow the current trajectory of fragmentation to continue, entrenching incompatible AI systems and regulatory silos that favour powerful incumbents over innovative competitors and impose mounting costs on organizations seeking to operate across jurisdictions. Alternatively, they can embrace the coordinated approaches outlined in this brief and following report, drawing on historical lessons to design adaptive frameworks that evolve with technology, establish early standards, build trust through robust verification mechanisms, and bridge technical and regulatory divides through multi-stakeholder collaboration. The sectoral roadmaps presented here provide actionable pathways for making this choice, with phased implementations, concrete success metrics, and clear responsibilities for each stakeholder group. The time to act is now, before fragmentation becomes irreversible and the opportunity to shape globally interoperable AI governance is lost.

ceimia