GLOBAL DATA ALLIANCE
TRUST ACROSS BORDERS

Promoting Digital Sovereignty

Building Capability, Collaboration, Resilience, and Trust Into Digital Ecosystems

Governments around the world are raising thoughtful questions about digital sovereignty as AI, cloud computing, and cybersecurity become central to economic growth and public services in sectors that include the aerospace, agriculture, automotive, finance, health, media, and telecommunications.

The Global Data Alliance (GDA)[1] submits that digital sovereignty should be understood as the ability to build and sustain a digital ecosystem based on **capability, collaboration, resilience, and trust.** These pillars can help governments govern, secure, operate, and recover critical digital systems while maintaining access to innovation, investment, and advanced technologies. The objective is to help governments achieve security, autonomy, and appropriate sovereign control while preserving access to global technology and data.

Achieving these objectives depends on open and interoperable digital governance policies. Cross-border data and investment flows support jobs, innovation, and public welfare across sectors. By contrast, data localization mandates, unnecessary restrictions on cross-border data transfers, and nationality-based restrictions on trade and investment can undermine the capability, collaboration, resilience, and trust upon which technology sovereignty depends.

WE URGE ECONOMIES TO EVALUATE HOW TO STRENGTHEN THEIR DIGITAL ECOSYSTEMS BY:

PILLAR I

Strengthening capability through investments in infrastructure, innovation, and skills

PILLAR II

Promoting industry-government and government-to-government collaboration

PILLAR III

Building resilience and redundancy into digital ecosystems

PILLAR IV

Promoting trust while safeguarding access to knowledge, information, and technology

Capability, collaboration, resilience, and trust are the building blocks of technology ecosystems that are sovereign and secure for the long term.

[1] The Global Data Alliance is a cross-industry coalition of companies committed to high standards of data responsibility and to respecting each economy's digital sovereignty. GDA members depend on the ability to securely share information and access knowledge and technology across borders to innovate and create jobs. The GDA supports policies that build trust in the digital economy while safeguarding cross-border data transfers and avoiding data localization requirements and nationality-based digital trade barriers.

PILLAR I

SOVEREIGNTY THROUGH CAPABILITY

Capability is a foundation of long-term digital sovereignty. Governments can strengthen it by investing in human capital, technical infrastructure, R&D, and international technology partnerships.

Global capability centers, startup ecosystems, academic institutions, and public-private partnerships can further strengthen domestic engineering, cybersecurity, AI, and cloud expertise while integrating local talent into global value chains.

Such investments depend on factors including:

- Connectivity to globally distributed cloud-computing capacity;
- Cross-border access to knowledge, information, and data;
- Integration of AI and other transformative tools into finance, health, manufacturing, and other sectors;
- Digital upskilling for researchers, programmers, engineers, technicians, and other professionals; and
- Engagement with governments and international institutions on interoperable digital governance frameworks.

PILLAR II

SOVEREIGNTY THROUGH COLLABORATION

Digital sovereignty depends on collaboration. Strategic partnerships can strengthen technological capacity, competitiveness, productivity, and security.

Collaboration occurs at several levels. Domestically, central and sub-central governments, industries, and communities collaborate to ensure that digital ecosystems are secure and responsive to local and national needs and interests. International standards organizations, industry, and technical experts collaborate to develop standards and technical specifications that are risk-based, effective, and interoperable. In bilateral, regional, and multilateral settings, national governments collaborate to avoid arbitrary, discriminatory, disguised, or unnecessary barriers to cross-border data transfers or to continuity of access to knowledge and technology, including barriers that modify conditions of competition to the detriment of foreign suppliers or restrict cooperation on the basis of origin.

Outward-oriented economies demonstrate the value of building sovereign strength through openness, innovation, talent, and collaboration. International initiatives such as the Organisation for Economic Co-operation and Development's Data Free Flow with Trust workstream, Pax Silica, the Hiroshima AI Process, and bilateral and regional digital trade agreements likewise demonstrate the value of cooperation on complex digital policy challenges.

PILLAR III

SOVEREIGNTY THROUGH RESILIENCE

Resilience is a core component of sovereignty. Critical digital systems should be able to withstand and recover from cyber incidents, natural disasters, infrastructure failures, and geopolitical disruptions.

Governments and enterprises have long used contingency planning and internationally recognized standards to benchmark readiness, redundancy, responsiveness, and recovery capacity. Multi-cloud architectures, hybrid deployment models, disaster recovery systems, portability norms, and open, interoperable standards can also reduce single points of failure and improve continuity.

These practices reflect a key insight: digital resilience benefits from diversity and choice across providers and technologies. Rather than concentrating risk in a single provider, technology stack, or infrastructure model, sovereignty frameworks should support choice, continuity, and contingency planning; restrictive, origin-based mandates can undermine these objectives.

PILLAR IV

SOVEREIGNTY THROUGH TRUST

Many sovereignty concerns are ultimately questions of trust: whether sensitive data and systems are secure, access is appropriately controlled, risks are auditable, and legal accountability mechanisms are effective. Encryption, key management, identity and access controls, auditability, contractual commitments, certification frameworks, and other technical and legal safeguards can provide these assurances without relying principally on geographic restrictions.

RECOMMENDATIONS

Sovereignty initiatives are more likely to achieve their objectives when built on capability, collaboration, resilience, and trust, and when they work with market incentives rather than against them. Constructive approaches include:

- Encouraging investment in capability and innovation through worker upskilling, non-discriminatory R&D incentives, support for technology entrepreneurship, high-performance computing, and publicly accessible digital infrastructure;
- Institutionalizing collaboration with governments and industry while supporting an open, pro-competitive digital ecosystem free from arbitrary, discriminatory, disguised, or unnecessary investment, trade, or data transfer restrictions;
- Using outcome-based public procurement to preserve access to best-in-class technologies;
- Promoting interoperability through voluntary, industry-driven standards for data, cybersecurity, and supply-chain risk management;
- Using encryption and privacy-enhancing technologies to protect sensitive data without unnecessary geographic restrictions; and
- Building trust through governance, transparency, legal safeguards, and early-warning and consultation mechanisms between trading partners to manage cross-border service risks, including continuity of access commitments.

Governments should avoid blanket, origin-based exclusions, including prescriptive procurement mandates that undermine competition, reduce technological capacity, and limit user choice. Such mandates can impede the cross-border investment and innovation that support productivity across the economy.

CONCLUSION

By focusing on capability, collaboration, resilience, and trust, governments can strengthen digital sovereignty while preserving access to innovation, investment, global technology partnerships, and the cross-border data flows on which modern digital ecosystems depend.