

## **DIGITAL SOVEREIGNTY RECOMMENDATIONS**

### **SUBMITTED TO G20 MEMBER TRADE AND DIGITAL MINISTERS**

August 2026

The Global Data Alliance is a cross-sector coalition of companies that depend on the ability to access and transfer data across borders to innovate and create jobs. Our members are active across agriculture, automotive, aviation, biopharmaceutical R&D, energy, finance, healthcare, manufacturing, media, supply chain, and telecom and other networking sectors. We offer these recommendations for consideration by G20 Ministers responsible for innovation, trade, and investment, building on the G20 AI Principles (Tsukuba, 2019) and subsequent G20 digital economy outcomes. We recommend language along the following lines.

**Opportunity.** We welcome the transformational potential of artificial intelligence and other emerging technologies to raise productivity, strengthen cybersecurity and critical infrastructure resilience, accelerate drug discovery and improve patient outcomes, expand financial inclusion, and enable micro, small, and medium-sized enterprises to reach customers worldwide. These gains depend on secure, high-performance connectivity; trusted cross-border data flows; and access to interoperable digital networks and tools that are connected, compatible, and able to work across borders and technology platforms to support AI workloads at scale. They accrue principally not to those who build frontier technology, but to the farmers, manufacturers, hospitals, insurers, public institutions, and small businesses that adopt it.

**Challenges.** Realizing these benefits requires an active and cooperative approach to the accompanying challenges. These include labor market transitions and the need for large-scale reskilling; cybersecurity and the resilience of critical systems; trusted access to cloud, network, and data infrastructure; and persistent divides in cross-border access to data, connectivity, compute, and skills. Cooperation among G20 members remains the most effective response to these challenges.

**Sovereignty through capability, collaboration, resilience, and trust.** We affirm the sovereign right of each member to regulate its own market, to invest in domestic capability, and to protect its essential security interests. Digital sovereignty is best understood as the ability to govern, secure, operate, and recover critical digital systems while retaining access to innovation, investment, trusted connectivity, interoperable infrastructure, and advanced technologies — built on four pillars: capability, collaboration, resilience, and trust. Requirements that are risk-based, proportionate, technology-neutral, and narrowly tailored to legitimate public policy objectives coexist most readily with an open and competitive digital market, preserve flexibility for AI and other data-intensive workloads, and support resilient access to global digital infrastructure.

We urge members to refrain from arbitrary, discriminatory, or unnecessary restrictions on digital trade, cross-border data transfers, continuity of access to technology, or the ability to access or deploy secure and resilient

infrastructure. These include measures that: (1) condition market access, certification, or public procurement on the nationality, ownership, headquarters, or country of origin of a supplier or its personnel; (2) require that data, computing facilities, or network management activities be located domestically absent a demonstrated and narrowly tailored risk; or (3) mandate that suppliers must be immune from another member's law. Such blanket exclusions, based on provider origin rather than demonstrated risk, reduce competition, raise costs, slow the diffusion of AI across the wider economy, fragment trusted digital infrastructure, and weaken the very capability, resilience, and trust that sovereignty frameworks seek to build, while failing to deliver commensurate benefit to national security. They fall hardest on economies without domestic alternatives and on smaller firms.

**Recommendations.** In this regard, we encourage members, on a voluntary and non-binding basis, to:

1. **Ensure continuity of service, connectivity, and access.** Refrain from measures that interrupt continuity of lawful access to digital products, services, network connectivity, data, computing capacity, and technologies supplied to or by other members, and provide advance notice and consultation where such action becomes unavoidable;
2. **Avoid discrimination.** Refrain from conditioning compliance with national standards, eligibility for government procurement, or the conduct of business on criteria that afford less favorable treatment to suppliers of other members – including the origin of a product or service, the nationality of a supplier or its personnel, the location of data, computing facilities, network infrastructure, or network operations, or a requirement that a supplier be immune from another member's law. Procurement criteria should be performance-, outcome-, security-, resilience-, and capability-based rather than focused on nationality or origin;
3. **Foster technology adoption and AI readiness.** Recognize that non-discriminatory and WTO-consistent loans, grants, and other support, workforce upskilling, research funding, digital infrastructure investment, secure connectivity, and publicly accessible high-performance computing can play a beneficial role in building domestic technological capacity and enabling responsible AI adoption;
4. **Early warning and consultation.** Notify other members of proposed measures affecting digital products, services, data flows, connectivity, computing capacity, or critical digital infrastructure; allow a meaningful opportunity for comment; and enter into consultations on request, so that service continuity, security, and resilience risks are managed cooperatively; and
5. **Anchor assurance in international standards and interoperable governance.** Base resilience, continuity, security, and AI assurance requirements on voluntary, industry-driven, internationally recognized standards and risk-management frameworks – such as ISO/IEC 27001, ISO/IEC 27031, ISO 22301, and the NIST AI Risk Management Framework – applied on a risk-based and technology-neutral basis rather than on origin-based criteria, so that suppliers are assessed on demonstrated performance, security, resilience, and responsible deployment.

**Conclusion.** Members are right to invest in their own technological capability. The Global Data Alliance urges that G20 members pursue this through the instruments that build capacity – investment, skills, interoperable infrastructure, open standards, and competitive markets – rather than through measures that substitute the nationality of a supplier for an assessment of risk. By building on capability, collaboration, resilience, and trust, economies can strengthen strategic autonomy, enable responsible AI adoption, and continue to benefit from global technology partnerships. We stand ready to provide technical expertise and economic data in support of this work.