



GLOBAL DATA ALLIANCE

TRUST ACROSS BORDERS

RECOMMENDATIONS ON SOVEREIGN AI CAPABILITY

SUBMISSION TO THE JOINT SELECT COMMITTEE ON ARTIFICIAL INTELLIGENCE

The Global Data Alliance (GDA)¹ is pleased to offer the following response to the recent inquiry of the Parliament of Australia's Joint Select Committee on Artificial Intelligence ("the Committee"). This submission focuses on paragraphs (e) – (f) of the Committee's Terms of Reference: Australian sovereign Artificial Intelligence ("AI") capability and Australian data sovereignty.

Executive Summary

The GDA supports the Committee's objective of strengthening technological and data-related sovereignty. In that regard, we encourage the Committee to distinguish between sovereign capability – the practical ability to govern, secure, operate and recover AI-enabled systems, while developing domestic skills, research and commercial capacity – and technological isolationism or technological exclusion.

For purposes of Term of Reference (e), we submit that "AI sovereignty" is best understood as the ability to build an AI ecosystem grounded in four pillars: capability, collaboration, resilience, and trust.² Conversely, isolationist or exclusionary policies keyed to technology origin, personnel citizenship, headquarters location, or other proxies for nationality – rather than to performance- and outcome-based metrics – narrow the range of providers and architectures available to Australian customers, reduce knowledge-sharing and technology-transfer opportunities, concentrate operational risk, and impede systematic safeguards and redundancies on which AI sovereignty depends.

For purposes of Term of Reference (f), data sovereignty should principally mean effective control over data – including access, security, governance, auditability and accountability – rather than a requirement that data be stored or processed exclusively within Australia.

We offer the following recommendations for how Australia can strengthen the former without removing itself from global technology, investment, research and data networks.

1. Sovereignty through Capability: Strengthen AI infrastructure, AI innovation, and AI skills;
2. Sovereignty through Collaboration: Promote sovereignty via industry-to-industry, industry-to-government, and government-to-government collaboration across AI domains;
3. Sovereignty through Resilience: Build resilience and redundancy into Australia's AI ecosystem; and
4. Sovereignty through Trust: Promote trust in AI governance while preserving the open, cross-border data flows that support AI development, deployment, and integration across the economy.

Discussion: Australian Sovereign AI Capability and Data Sovereignty

Terms of Reference paragraphs (e) and (f) address the following questions:

- (e) the opportunities for Australian sovereign AI capability, including the measures required to build, retain and commercialise domestic capability, grow research and development, and attract and retain investment and talent;
- (f) the importance of data sovereignty, and the opportunities presented by narrow, domain-specific AI models trained on Australian data in areas of Australian sectoral expertise.

We address both priorities through the four recommendations below.

Recommendation 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.

The most durable sovereign capabilities include people, institutions, infrastructure, research capacity, and high-quality data assets. For AI, priority areas include AI and cybersecurity skills; access to high-performance compute; cloud and data engineering; research and development; standards expertise; model evaluation; data curation; and pathways that help Australian research and start-ups reach commercial scale.

Australia starts from a meaningful base. The National AI Plan notes that Australia attracted A\$700 million in private investment in AI firms in 2024 and that demand for AI-skilled workers has tripled since 2015. Policy should build on that momentum by making Australia an attractive place to conduct research, deploy engineers, establish capability centres, develop products, and scale firms.

For example, Australia's 2026 Expectations for data centres and AI infrastructure developers provide a useful illustration of this approach. They call on providers of large-scale compute to contribute to Australian skills and research, including by: (1) enabling compute access for Australian start-ups, innovative small businesses and researchers, and (2) deploying engineers and researchers in Australia. This is a constructive model for sovereign capability: use investment to expand Australian skills, computational capabilities, research capacity rather than treating international participation as inconsistent with sovereignty.

Broadly speaking, development of such capabilities depends on factors including:

- Cross-border access 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 standards organizations on interoperable governance frameworks.

We urge the Committee to ensure that any recommendations relating to sovereign capability do not compromise these success factors.

Recommendation II: Sovereignty Through Collaboration

Sovereign AI in Australia also depends on the type of industry-to-industry, industry-to-government, and government-to-government collaboration that can sharpen technological competitiveness, productivity, and security.

As an illustration of **industry-to-industry collaboration**, Australian companies will often commercialise AI by adapting existing models and tools to Australian problems rather than by recreating every layer of the AI stack. The Productivity Commission has identified an important near-term opportunity for Australia in adapting general-purpose models to specific local use cases and in developing models that can be trained on smaller, high-quality datasets. This observation is directly relevant to Terms of Reference (e) and (f).

To pursue that opportunity, Australian researchers and firms need reliable access to complementary inputs that are often globally distributed: accelerated compute, base and foundation models, cybersecurity services, specialised enterprise software, and research partners. Restricting these inputs by nationality or ownership can raise entry costs and make it harder for Australian firms to achieve commercialisation.

Government-to-industry collaboration can explore approaches to support interoperability, portability and competitive access. Australian firms should be able to choose among technologies and providers, combine domestic and international inputs, and change providers when business, security or resilience needs require it. These conditions support commercialisation while reducing dependence on any single technology, provider or architecture.

As an illustration of **government-to-government collaboration**, governments benefit from commitments to avoid arbitrary, discriminatory, disguised, or unnecessary restrictions on digital trade, cross-border data transfers, or continuity of access to technology. Outward-oriented economies demonstrate the value of building sovereign strength through openness, innovation, talent, and collaboration. International initiatives such as the OECD's Data Free Flow with Trust framework, Pax Silica, the Hiroshima AI Process, and bilateral and regional digital trade agreements likewise demonstrate the value of cooperation on complex digital policy challenges. Australia's own international practice reflects this approach. For example, the Australia-Singapore Digital Economy Agreement combines commitments supporting cross-border data flows and avoiding unnecessary localization requirements with practical cooperation on AI, data innovation, personal-data protection and digital standards.

To sustain and safeguard such collaboration, Australia's policy settings should therefore remain predictable, risk-based and non-discriminatory. Broad requirements that AI infrastructure, models or service providers be domestically owned or headquartered can work against these collaborative objectives. They may deter investment, reduce the range of available technologies and force Australian organisations to duplicate capabilities that can be obtained more efficiently through trusted partnerships. Outcome-based requirements – security, auditability, continuity, portability, access control and legal accountability – are better suited to testing whether a service advances Australian interests.

Recent Oxford Economics modelling underscores what is at risk when sovereignty measures move from performance-, accountability-, and assurance-based criteria to broad origin-based restrictions. Modelling five levels of AI sovereignty restrictiveness across the Asia-Pacific, the study found that costs and risks rise non-linearly when origin-based restrictions are imposed in place of functional performance-based criteria.

While Australia was not included in the study, the regional results nevertheless support caution. For example, at the most restrictive levels, firm-level AI adoption in Japan would fall from a projected 20.3% to 3.4% by 2035, with total opportunity costs exceeding US\$58 billion (1.4% of 2035 GDP); in Singapore, adoption would fall from 43.8% to 9.6%, at an opportunity cost of 3.2% of 2035 GDP.³ These results illustrate the types of trade-offs — including higher costs, slower AI diffusion and lower productivity — that warrant careful Australia-specific assessment before broad origin-based sovereignty requirements are adopted.

Recommendation III: Sovereignty Through Resilience

Resilience is a core component of sovereignty. For purposes of sovereign AI capability, the relevant question is whether critical digital systems can withstand disruption, continue performing essential functions, and recover within defined timeframes. Cyber incidents, infrastructure failures, natural disasters, supply-chain disruptions and geopolitical events can arise regardless of where a technology provider is headquartered or where particular infrastructure is located.

Australia already provides a useful model for assessing resilience through operational outcomes. APRA Prudential Standard CPS 230 requires regulated entities to maintain critical operations within defined tolerance levels through severe disruptions, maintain credible and regularly tested business-continuity plans, and manage risks associated with material service providers. APRA specifically calls for testing against “severe but plausible” scenarios and for regulated entities to understand and manage their dependencies on service providers. This is a useful model for sovereign AI: resilience is assessed by whether critical functions

can withstand and recover from disruption, rather than principally by the nationality or headquarters location of the technology provider.

Other Australian frameworks reinforce this approach. The Security of Critical Infrastructure risk-management framework takes an all-hazards approach encompassing cyber and information-security, personnel, supply-chain, physical-security and natural hazards. The Australian Signals Directorate's Essential Eight likewise treats secure backups and tested restoration as elements of cyber resilience. The significance of these frameworks is not that every AI deployment should be subject to identical requirements, but that Australia already evaluates resilience through measurable operational outcomes rather than nationality or origin.

Internationally recognised standards provide additional benchmarks for evaluating these capabilities. ISO 22301:2019, the international standard for business continuity management systems, addresses preparedness for, response to and recovery from disruptive incidents. ISO/IEC 27031:2025 provides more specific guidance on ICT readiness for business continuity, including restoration of ICT services within agreed timeframes and management of dependencies on third-party services. ISO/IEC 27001:2022 provides a complementary framework for managing information-security risks and maintaining the confidentiality, integrity and availability of information. For cloud environments, ISO/IEC 27017:2026 provides additional guidance concerning cloud-specific security controls. Collectively, these frameworks point to relevant resilience indicators such as tested business-continuity and disaster-recovery arrangements; recovery-time and recovery-point objectives; secure backups; technical and geographic redundancy; tested failover; portability and exit arrangements; incident-response procedures; visibility into important third-party dependencies; and the capacity to substitute providers or technologies where necessary.

Multi-cloud architectures, hybrid deployments, geographically distributed infrastructure, interoperable standards and portability mechanisms can all contribute to these objectives. Not every organisation will need every architecture, and resilience requirements should remain proportionate to the risk and importance of the workload. But policies that unnecessarily restrict the available set of providers or technologies can have the opposite effect: they can reduce architectural choice, make substitution more difficult and concentrate dependencies rather than diversify them.

Taken together, these Australian frameworks and internationally recognised standards point toward a practical model for sovereign AI. Accordingly, the GDA encourages the Committee to treat tested continuity, redundancy, recoverability, portability, and supplier-risk management as more meaningful indicators of sovereign resilience than nationality or origin.

Recommendation IV: Sovereignty Through Trust

Many concerns expressed through the language of data or AI sovereignty are ultimately questions of trust: whether sensitive data is protected; whether access can be effectively controlled; whether system behaviour and risks can be assessed; whether providers can be audited and held accountable; and whether Australian organisations retain meaningful control over their data and systems.

These objectives can increasingly be evaluated against recognised technical, governance and assurance frameworks. AS ISO/IEC 42001:2023, which Standards Australia adopted identically from the international ISO/IEC standard, provides a management-system framework for responsible AI governance, including risk management, accountability, traceability, transparency and reliability. Australia has expressly aligned its AI guardrails with the NIST AI Risk Management Framework, explaining that international consistency is particularly important for Australia as an trading economy and can help avoid unnecessary barriers to firms operating across markets.

For data sovereignty in particular, effective control does not generally require exclusive domestic storage or processing. Encryption, customer-controlled key management, identity and access controls, data classification, audit logs, contractual limits on access, independent assurance, incident-management

procedures, privacy protections and enforceable accountability can provide strong mechanisms for protecting Australian data while permitting use of globally distributed digital infrastructure.

Australian privacy law itself illustrates this distinction. Australian Privacy Principle 8 generally requires an Australian entity disclosing personal information overseas to take reasonable steps to ensure that the overseas recipient does not breach applicable Australian Privacy Principles, and in defined circumstances makes the Australian entity accountable for the recipient's conduct. The framework therefore focuses substantially on responsibility and accountability for data transferred abroad, rather than establishing a general requirement that personal information remain physically within Australia.

This distinction is particularly relevant to the Committee's interest in domain-specific models trained on Australian data. Australia can strengthen sovereign capability by improving the quality, governance, provenance and availability of Australian datasets in areas such as agriculture, resources, medical research, advanced manufacturing and financial services. Trustworthy use of those datasets should include appropriate permissions, documentation, access controls, provenance, security and auditability. But those objectives do not require the complementary compute, foundation models, cybersecurity services, software or research expertise used with the data to originate exclusively in Australia.

For classified military, intelligence, or other highly sensitive government information, a specific risk assessment may justify additional location or access restrictions. Outside those narrow circumstances, however, the better test is whether Australia can control access, verify security, enforce accountability and maintain operational control. International standards, independent assurance and measurable technical safeguards can provide more precise evidence of those outcomes than the headquarters, nationality or ownership of the technology provider.

Conclusion

The Committee has an opportunity to give 'sovereign AI capability' and Australian 'data sovereignty' practical meaning.

The GDA's Digital Sovereignty Position Paper proposes four mutually reinforcing pillars: capability, collaboration, resilience and trust.

This approach focuses on sovereignty in terms of performance-based metrics to assist government, enterprise, and communities adopt and address the opportunities and challenges that AI presents – rather than as a narrow nationality or origin test.

This is a framing consistent with Australia's National AI Plan, which expressly pairs support for domestic AI capability with the attraction of global investment. That combination is important: a policy designed to strengthen local capability should not unintentionally narrow access to the investment, technologies and expertise needed to build it.

The GDA appreciates the opportunity to raise these points and would welcome the opportunity to appear before the Committee or to provide further information on the matters raised above.

¹ The GDA is a cross-industry coalition of companies that are committed to high standards of data responsibility and that rely on the ability to access and transfer information across borders to innovate and create jobs. GDA member companies are active in the accounting, agriculture, automotive, aerospace and aviation, biopharmaceutical, consumer goods, energy, film and television, finance, healthcare, hospitality, insurance, manufacturing, medical device, natural resources, publishing, semiconductor, software, supply chain, telecommunications, and transportation sectors. Many GDA members are longstanding investors, employers, and taxpayers in Australia. For more information, see <https://www.globaldataalliance.org>

² Global Data Alliance, Promoting Digital Sovereignty: Building Capability, Collaboration, Resilience, and Trust into Digital Ecosystems (2026), available at <https://globaldataalliance.org>.

³Oxford Economics for the AI Adoption Initiative, The Economics of Sovereign AI: Balancing Autonomy, Innovation, and Growth in the Asia-Pacific (May 2026), Figures 3, 24 and 25.