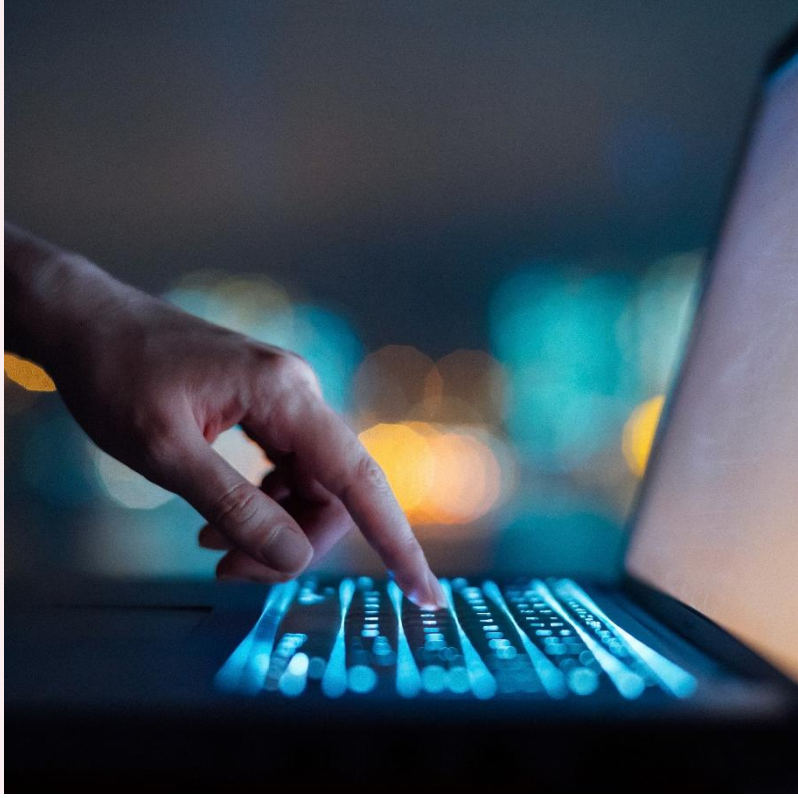
Clifford Chance

BRIEFING



AUSTRALIA'S NATIONAL AI PLAN 2025: KEY TAKEAWAYS

29 January 2026

Contents

- **Australia is positioning AI and digital infrastructure as national strategic priorities**, with strong government facilitation for data centre investment and an emphasis on aligning projects with national interest objectives such as security, sustainability, renewable energy, and economic growth.
- **Regulation will tighten, but through targeted reforms, not a standalone AI law.** The Plan signals increased expectations on responsible AI governance, privacy, safety and transparency, requiring businesses to adapt to evolving standards and demonstrate compliance across the AI lifecycle.
- **Data centres sit at the heart of Australia's AI ambition**, with new national principles, streamlined approval pathways and sustainability expectations that will shape how facilities are planned, built, powered, secured, and operated.
- **Global alignment matters, but local requirements will still drive operational decisions.** Organisations operating in Australia must navigate local privacy, cybersecurity, critical infrastructure and data governance obligations while keeping pace with emerging international standards and best-practice frameworks.

EXECUTIVE SUMMARY

The National AI Plan 2025 (the Plan) was released by Australia's federal government on 2 December 2025.

It sets out Australia's strategy to capture AI opportunities – by building smart infrastructure, backing domestic capability and attracting investment – while spreading the benefits and keeping Australians safe through robust legal and ethical frameworks and international engagement. The Plan takes a whole-of-economy approach and is closely aligned with Australia's broader industrial strategy (Future Made in Australia).

Data centres are central to the AI ecosystem, providing critical infrastructure for AI model training, deployment and service delivery. The Plan details policy priorities, regulatory settings and investment facilitation measures that are directly relevant to data centre investors whether in their capacity as financiers, equity investors, developers, operators or customers (as applicable).

While the Plan itself does not create new legal obligations, it signals the direction of travel for regulation, investment, and government procurement in Australia. The Plan suggests a more proactive regulatory environment, with increasing expectations for responsible AI governance, transparency, and alignment with national interests.

Similar to the UK (which published their "AI Opportunities Plan" in January 2025) Australia's approach appears to be risk-based, leveraging existing laws and targeted reforms rather than introducing a standalone AI law such as the EU AI Act. While the government is committed to international alignment (including through the G7 and bilateral partnerships), global companies may need to tailor their AI products and governance to meet Australian privacy, copyright, and online safety requirements.

1. GOVERNMENT SUPPORT FOR DATA CENTRE INVESTMENT

Summary: Australia is positioning itself as a leading destination for data centre investment in the Indo-Pacific because of its stable operating environment, clear legal protections, abundant renewable energy potential, available land, proximity to growing economies, access to advanced chips and connectivity through international submarine cables. The government will support data centre investment through the development of national data centre principles and infrastructure planning. Additionally, it will facilitate regulatory approvals for data centres and their associated energy sources through existing initiatives such as the Investor Front Door and the Major Project Facilitation Agency (MPFA).

Key Takeaways:

- Government support focuses on enabling nationally significant projects that align with forthcoming national data centre principles, using facilitation (Investor Front Door/MPFA) to identify and address approval barriers and to coordinate with states and territories where alignment is demonstrated.
- Data centre developers and operators should engage early with agencies such as the Investor Front Door and Major Project Facilitation Agency to explore opportunities to expedite approvals for their new data centre projects. For example, when planning a new facility, these parties should proactively seek guidance from these agencies to identify and address regulatory barriers, as the government is actively working to make it easier to develop major, transformational projects and invest in Australia.
- Data centre developers and operators should highlight their alignment with national priorities (such as supporting local jobs, using renewable energy, and contributing to digital infrastructure) and improving compute capacity and connectivity (which are two critical components for AI at scale) in their project proposals to increase the likelihood of government support and streamlined approvals.
- Additionally, the government is exploring opportunities to unlock high value datasets for pilot AI use cases, from both public and private sources which may create opportunities for data sharing and licensing but also heightens the importance of having robust privacy, IP and data controls in place.

2. NATIONAL DATA CENTRE PRINCIPLES AND REGULATORY COORDINATION

Summary: The government will develop a set of national data centre principles, in partnership with the states and territories, to clarify the expectations for data centres that align with Australia's national interests. These principles will include clear guidance on sustainability, security, and other factors such as bringing new renewable energy online and adopting efficient cooling technologies. Where data centre developers and

operators demonstrate alignment with these principles, their projects may be subjected to a streamlined approval process.

Key takeaways

- Data centre developers and operators should design data centres to meet or exceed these national data centre principles, such as by integrating renewable energy sources (e.g., on-site solar or wind power purchase agreements) and adopting efficient cooling technologies (e.g., liquid cooling systems that reduce water consumption).
- Data centre developers and operators should establish internal compliance teams to monitor the development of these principles and flow through regulatory developments and adjust project plans accordingly to ensure that new builds and expansions are future proofed against evolving requirements.
- When seeking approvals, data centre developers and operators should prepare documentation demonstrating how their projects align with sustainability, security, and national interest criteria, which may facilitate faster and more predictable approval processes.

3. ENERGY, SUSTAINABILITY AND ENVIRONMENTAL REGULATION

Summary: Supporting sustainability, energy security and investment in clean technologies through data centre growth is a key objective within the Plan. Data centres are significant water and energy users. Australia's Energy Market Operator predicts the electricity demand from data centres will triple by 2030. Therefore, the government is seeking to leverage the AI infrastructure initiatives to accelerate Australia's renewable transition and promote investment in renewable energy.

Key takeaways

- Data centre developers and operators should incorporate energy efficiency and renewable energy targets into construction, procurement and operational contracts - for example by requiring contractors to use energy-efficient materials and systems, and negotiating green energy supply agreements for ongoing operations. These sustainability matters may also be important to financiers and equity investors in data centres.
- Data centre developers and operators should also engage early with energy market bodies and network services providers to manage and mitigate connection and grid impacts.
- Data centre developers and operators may implement water-saving technologies (e.g., closed-loop cooling systems) and track water and energy usage to ensure compliance with state and federal regulations.
- Environmental compliance clauses should be included in customer contracts, making clear the data centre's commitments to emissions standards and sustainability reporting, which can also be a selling point for attracting customers.

4. CRITICAL INFRASTRUCTURE, CYBERSECURITY AND NATIONAL SECURITY

Summary: The government is committed to coordinating cross-government efforts to uplift cybersecurity and safeguard critical infrastructure during the growth of AI. Part of this will include the Department of Home Affairs, the National Intelligence Community and law enforcement agencies monitoring the serious risks posed by AI development. The Plan also recognises that it is in Australia's interest, including for national security, to ensure AI development happens locally.

Key takeaways

- Data centre developers and operators should implement robust cybersecurity frameworks (such as ISO 27001 certification) and regularly update security protocols to meet or exceed government requirements for critical infrastructure.
- Depending on the nature of the data centre investment and its customer base, data centre developers and operators may wish to offer sovereign hosting / data residency to support Australian sovereignty objectives referred to in the Plan - for example by offering dedicated hosting environments for government or sensitive data that are physically and logically separated from other customers. This is a hot topic in many jurisdictions, including from an EU regulatory perspective. The government emphasised its commitment to upholding the principles of the Framework for Governance of Indigenous Data (NIAA 2024) ensuring that First Nations communities have control over the collection, access, use, and sharing of their data.

- Foreign investors should conduct regular reviews of their ownership structures and planned transactions to anticipate potential FIRB triggers and prepare for possible conditions or restrictions, such as requirements for Australian-based management or board representation and 'on shoring' of sensitive data and associated systems.

5. PRIVACY AND DATA GOVERNANCE

Summary: Privacy and data governance for AI systems in Australia will build on existing legal and regulatory frameworks and will be actively enforced and adapted to address emerging AI risks. Non-compliance may lead to the imposition of injunctions or civil penalties by regulators, or contractual remedies under the *Australian Consumer Law*. The government has identified several regulations to manage AI-related harms, including ongoing reforms to the *Privacy Act 1988* (Cth). One important reform is the recent introduction of the statutory tort for serious invasions of privacy. This tort enables individuals to seek redress for privacy harms in Court. The Plan also highlights the importance of robust data governance, privacy protections, documentation, human oversight and legal compliance to unlock Australia's data potential.

Key takeaways

- Customers of data centres should embed documentation, human oversight and legal compliance in privacy management programs in line with the Plan. This might involve regularly updating data security, planning cyber-security incident responses, developing systems for rapid notification of data breaches to affected individuals and the Office of the Australian Information Commissioner (OAIC) per the OAIC's Notifiable Data Breach scheme, and implementing mechanisms to obtain and manage customer consent.
- Regular privacy impact assessments should be conducted to identify and mitigate risks associated with new services or changes in data handling practices. These governance matters may also be important to financiers and equity investors in data centres.

6. EMERGING STANDARDS AND INTERNATIONAL ALIGNMENT

Summary: Businesses are expected to adopt AI responsibly by developing and using systems that are transparent, fair, accountable, and compliant with relevant laws. On 15 December 2025, the government (digital department) published a new government policy on responsible AI use in government / public sector. Although the policy is aimed at government agencies, it may still be relevant to private sector investors because it sets a new benchmark for what is "responsible AI" in Australia. The government continues to engage in international AI governance and has signalled its commitment to various multilateral and bilateral agreements to uphold global standards. Finally, the Plan establishes a new AI Safety Institute (which is similar to the UK's Security Institute), signalling Australia is seeking to position itself as a global leader in AI safety.

Key takeaways

- Data centre developers, operators and customers (as applicable) should track and adopt relevant international and Australian standards (such as ISO 27001 for information security, ISO 50001 for energy management, and ISO/IEC 30134 for data centre resource efficiency) to ensure compliance and market competitiveness.
- These parties should participate in industry forums and standards development processes to stay ahead of regulatory changes and influence best practices. To this end, they may also wish to monitor the G7 Energy and AI Work Plan to understand new best practices and evolving expectations on powering AI/data centre reliability and cost efficiency, and how those requirements may impact their Australian investments.
- The policy for the responsible use of AI in government may provide guidance to private sector investors as to the best practices for AI governance frameworks. This policy requires the organisation to provide publicly available AI transparency statements; designate accountable officials for the AI; create internal registers of AI use cases and risk assessments; provide mandatory staff training on responsible AI; and proportionate risk mitigation and ongoing monitoring.

Nadia Kalic
Partner, Sydney

Email: nadia.kalic@cliffordchance.com
Mobile: +61 401450025

Robert Tang
Partner, Sydney

Email: Robert.Tang@cliffordchance.com
Mobile: +61 431084911

Reuben Van Werkum
Director, Sydney

Email: reuben.vanwerkum@cliffordchance.com
Mobile: +61 488300201

Chad Bohan
Partner, Sydney

Email: chad.bochan@cliffordchance.com
Mobile: +61 401783269

Stella Cramer
Partner, Singapore

Email: stella.cramer@cliffordchance.com
Mobile: +65 90111196

Matt Buchanan
Partner, Singapore

Email: matthew.buchanan@cliffordchance.com
Mobile: +65 91773126

Tom England
Partner, Singapore

Email: thomas.england@cliffordchance.com
Mobile: +65 96488352

Tom Capel
Counsel, Singapore

Email: Thomas.Capel@CliffordChance.com
Mobile: +65 83990481