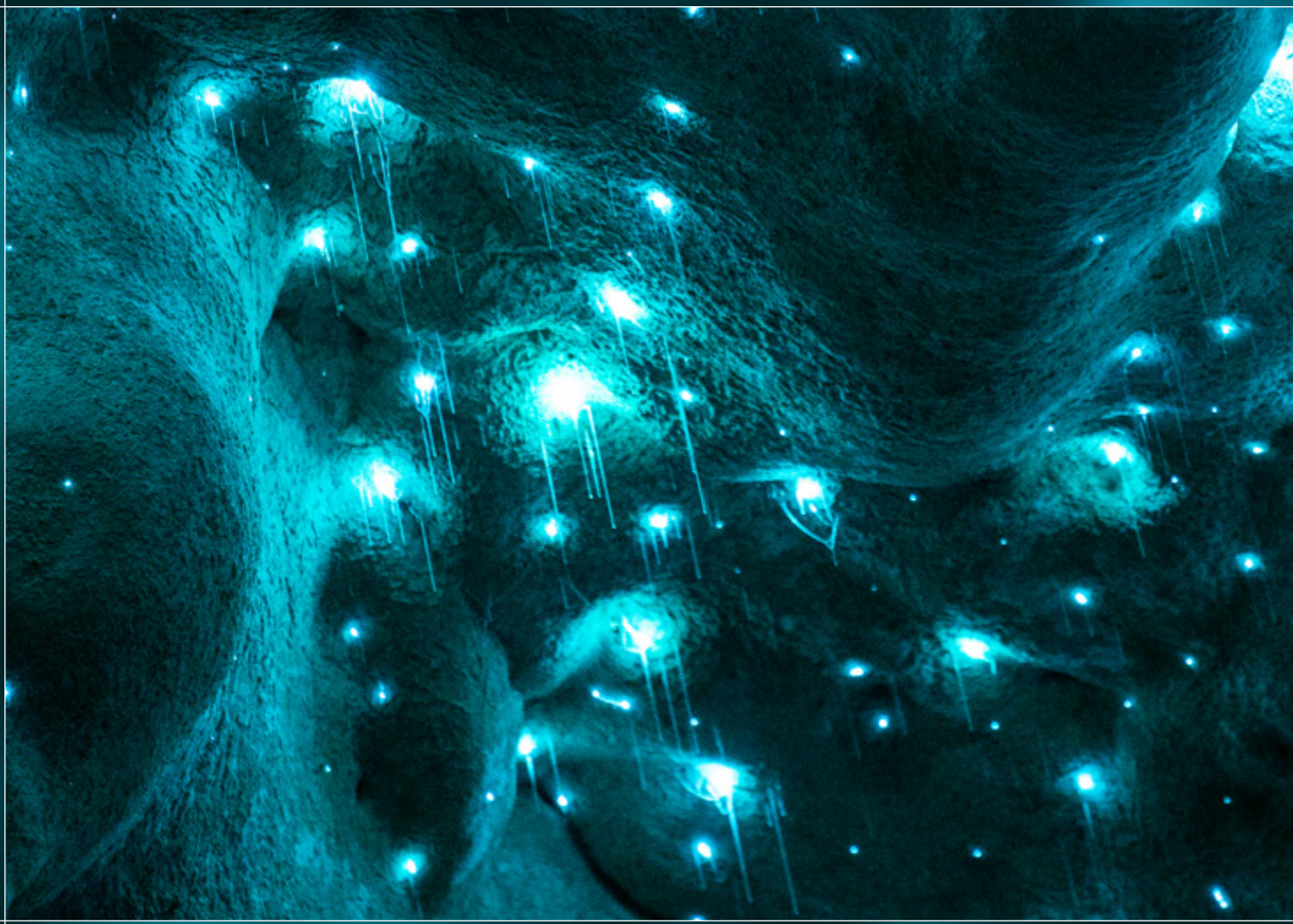
November 2026

Data Centres

APAC Regulatory Guide – **Australia**

Investment considerations



MALLESONS

Chapter 1

Australia



A year of... growing regulatory scrutiny, infrastructure constraints and heightened oversight

Population	Data centres	Live capacity	Pipeline capacity
27.8 million	279	1.63GW	5.7GW+
	YoY: 28 (11.2%)	YoY: 255MW (18.6%)	YoY: 2.5GW (79.4%)

Data centre statistics provided by DC Byte (as at September 2026)

Australia's data centre market is anticipated to double in the next 5 years. With its stable economy, transparent regulatory framework and robust infrastructure, Australia is a relatively safe location for data centre investment from a legal and regulatory perspective.

There is significant demand for on-shore data centre capacity (driven by hyperscalers and neoclouds) as a mature economy. The evolving legal framework for AI, including copyright issues, may influence the pace and nature of AI deployment.

The allure of the Australian market is marked by insufficient carrots and burdensome sticks. Australia's strict foreign investment regime can significantly affect the timing and structuring of site acquisitions, investments in data centres and tenancies involving foreign tenants.

Power transmission continues to be a concern. Critical infrastructure regulations and government security requirements increase the regulatory burden. Despite these impeding factors, a remarkable data centre growth story is emerging.

Opportunities

- Stable economy and abundant land
- Clear(er) regulatory landscape
- Relatively unrestricted access to advanced AI chips and model weights

Challenges

- Power supply constraints
- Foreign investment controls
- Competing requirements between Federal and State governments

Spotlight on key drivers

Stable economy with a clear regulatory landscape

With laws that clearly outline the relevant procedures for power and land approvals, developers and investors can navigate the permitting process and management of data centres with confidence. Although these requirements can prove burdensome and impose delays, they ultimately bring clarity that fosters trust among investors and positions Australia as a reliable hub for data centres in the APAC region.

The Australian Government has published national 'Expectations of data centres and AI infrastructure developers' (**Expectations**), providing guidance for how data centre operators and AI infrastructure developers may receive priority approval from regulators for their proposal. The government is also consulting on proposed mandatory standards for large data centres and AI training, with the States also seeking to set the 'rules of the road' for investment.

These settings may increasingly influence regulatory assessments and project development.

Power supply constraints

The progressive retirement of major coal power stations, combined with network capacity constraints and the skyrocketing energy demands of new data centres, is expected to place increasing pressure on power supply. The increased demand for data centres is also presenting challenges for connecting large new electricity loads.

Large data centre and AI infrastructure developers are increasingly expected to secure their own power supply and contribute to the costs of connecting new load to the electricity system. In Victoria, new data centres will be expected to match new demand with new renewable generation and storage, and meet associated connection and network upgrade costs.

Foreign investment hurdles

Chief among these is the requirement for FIRB approval from the Federal Treasurer for land acquisitions and data centre operations, along with the significant operational constraints imposed by the *Security of Critical Infrastructure Act 2018* (**SOCI Act**) and the Federal Government's Hosting Certification Framework (**HCF**). Reforms that are under way should lead to simpler treatment for genuinely low-risk investments, but data, AI and critical infrastructure investments are still likely to be closely scrutinised.

Developers and investors should carefully assess the FIRB, SOCI Act and HCF implications before committing to data centre projects in Australia, and for post-completion compliance obligations.

> Australia's compelling data centre investment story is increasingly challenged by power, infrastructure and approval constraints. Collaboration between government and industry is key to ensuring ongoing regulatory reform supports sustainable growth.
>
> Rachael Lewis
> Partner, Mallesons



01 Power

Getting power to a site

In Australia, there is limited choice when seeking a physical electricity connection. Electricity is provided by licensed network service providers (**NSP**). Each region typically only has one high voltage licensed NSP.

The connection process depends on the type of works, with non-contestable works performed by NSPs and contestable works being open to competition from multiple contractors.

Concerns include:

- the potential for insufficient power supply given the accelerating phase-down of large coal power stations (including Eraring Power Station, Australia's largest coal-fired generator, scheduled to close in April 2029) and the forecasted massive energy consumption requirements of new data centres, and
- some parts of the NSPs' networks that are at capacity, creating constraints on where large new electricity loads can be connected.

6–12 month negotiation process (typically)



Data centre submits 'connection enquiry' with relevant NSP

Who undertakes works?

Non-contestable works - performed by the NSP
Contestable works - open to competition from multiple contractors

Early works possible

In some cases, limited power connection works may start before arrangement finalised

Connection arrangement agreed

National expectations and standards for data centres and AI training

The Australian Government published its Expectations in March 2026, as part of the National AI Plan released in December 2025. The Expectations form part of the sector's social licence to operate in Australia. Projects most closely aligned with those expectations will be prioritised in regulatory assessments.

Five core national Expectations will apply to new or expanded data centre developments within Australia:

1. prioritising Australia's national interest
2. supporting Australia's energy transition
3. using water sustainably and responsibly
4. investing in Australian skills and jobs, and
5. strengthening research, innovation and local capability

The Government expects energy-intensive developments, including data centres and AI infrastructure, to fund an appropriate share of the transmission and distribution infrastructure costs associated with connecting new load to the electricity system.

Building on the Expectations, the Government released a Consultation Paper, proposing mandatory national standards for large data centres and AI training, on 17 September 2026. The proposed standards would address energy, water and land use, local jobs and capability, along with conditions for AI training. Power-related implications include that data centres fund an appropriate share of transmission and distribution infrastructure costs.

Although this sits within power, the proposals are cross-cutting and may affect project feasibility, approvals and ongoing operations.

Large data centre developers should factor network contribution costs into project feasibility from the outset. Developers and investors should monitor ongoing consultations and consider how proposed projects align with the emerging standards.

Power purchase agreements

In Australia, most corporate PPAs are structured as corporate virtual PPAs (also known as 'contracts for difference' or 'synthetic PPAs') rather than corporate physical PPAs.

The increasing adoption of 24/7 carbon-free energy (**CFE**) procurement targets by major technology companies is driving a shift towards more sophisticated time-matched PPA structures, supported by advances in granular energy certificate tracking.

While it is technically possible to structure a corporate physical PPA if the generator is on site and connects directly to the data centre, it is not generally possible for a consumer to acquire electricity directly from a generator if the electricity needs to be wheeled through the grid.

In these scenarios, electricity must be bought and sold through the central market, operated by the Australian Energy Market Operator (**AEMO**).

In some circumstances, a corporate virtual PPA can also be considered a financial derivative.

Depending on how the corporate virtual PPA is structured, and how many virtual PPAs are entered into, parties may be required to hold an Australian financial services licence or organise an intermediary relationship with a person who holds such a licence.

NABERS

Certified sustainability ratings are provided by the National Australian Built Environment Rating System (**NABERS**), which influences where data centres are built, and how efficiently they must operate to be eligible for government contracts and funding.

Only data centres with a 5-star NABERS rating are eligible to join the Data Centre Panel set up by the Australian Government's Digital Transformation Agency and undertake government work, under rules that commenced on 1 July 2025.

Renewable energy certificates

Buying and surrendering RECs based on the power used is an obligation for any data centre covered by the Australian Government's Renewable Energy Target (**RET**). This aims to reduce GHG emissions in the electricity sector and increase renewable electricity generation, capturing 'liable entities' - primarily electricity retailers and large energy users, which may include data centres.

The RET has been met ahead of schedule, and discussions are underway regarding successor schemes, including integration with the Safeguard Mechanism and potential data centre-specific renewable energy purchase obligations.

The future of the Retailer Reliability Obligation (**RRO**) is uncertain following the landmark 'Nelson Review' of National Electricity Market (**NEM**) wholesale market settings. Every NEM jurisdiction except Queensland has agreed in-principle to the core reforms recommended by the Review, including a proposed Electricity Services Entry Mechanism (**ESEM**).

The ESEM is intended to replace and evolve existing government underwriting schemes with a permanent, nationally consistent and market-linked mechanism to support new investment. It is currently in design, with implementation targeted by the end of 2027.

The RRO may also require those 'liable entities' to demonstrate that they hold sufficient firmed electricity contracts to cover a data centre's load in the event of forecasted supply shortfalls. AEMO has increased the frequency of reliability assessments in response to growing system stress events, and data centre operators should factor RRO compliance into procurement strategies.

Technical access standards in the NEM National Electricity Rules will apply consistently across data centres under recent revisions. These standards are designed to facilitate:

- faster and more efficient connection process
- cost reductions in connection process, and
- enhanced reliability and stability of power supply.

These revisions categorise connection applications based on type rather than owner or operator registration.

Capacity Investment Scheme

The government's Capacity Investment Scheme (**CIS**) provides underwriting support for new renewable generation and storage capacity. Data centre operators may indirectly benefit from the CIS by entering offtake arrangements with CIS-supported projects, which can provide access to competitively priced renewable energy with government-backed revenue certainty for generators.

The scheme has expanded from its initial scope and now includes Variable Renewable Energy (**VRE**) tenders and Clean Dispatchable Power (**CDP**) tenders.

Data centre developers should monitor CIS tender outcomes as a source of potential PPA counterparties. The proposed ESEM is expected to replace the CIS as the primary mechanism for supporting investment in new generation, storage and firming capacity. Subject to detailed design and legislative implementation, the ESEM would provide a permanent, nationally consistent and market-based framework for supporting new investment.

Behind-the-meter generation and storage

Data centres are increasingly exploring behind-the-meter (**BTM**) renewable generation and BESS to manage both energy costs and grid connection constraints.

BTM assets can reduce reliance on grid capacity, provide backup power, and in some configurations enable participation in the NEM's wholesale market or ancillary services markets.

Regulatory treatment of embedded generation continues to evolve, with recent reforms clarifying the obligations of embedded network operators. Proponents should carefully assess network service provider requirements and embedded network licensing obligations when planning BTM installations.

02 Water

Water supply

A new data centre development will require a consent to connect to the relevant water authority's existing water infrastructure assets.

There are approximately 196 businesses and local governments which provide water services, and each authority has its own connection policies and connection contracts for new customers.

High water demand customers may face further requirements. The existing system may not have capacity to cater for the development, or the demand on the system may adversely affect supply to existing customers.

A separate water licence, water entitlement or commercial agreement may be required in some situations, depending on the local jurisdiction. These arrangements may be for a set timeframe, or subject to a range of conditions.

New infrastructure to the site or an upgrade of the water authority's existing assets away from the site may be required by the data centre developer for a very high water demand. New connections and infrastructure development will be assessed for water efficiency, re-use and water use reduction opportunities.

Water laws, policies and guidelines

All developments, including data centres, must comply with general legal obligations relating to water, waste management and environmental and planning approvals. These obligations vary between each state, territory and local government.

As data centres are considered significant developments, planning approvals and environmental impact assessment in most locations include requirements for sustainable design and management information (including water efficiency and reuse).

> For example, in New South Wales (**NSW**), an Integrated Water Management Plan is required as part of the Environmental Impact Statement assessment process for data centres as a 'State significant development'. The plan must outline the necessary water-relating servicing infrastructure for the development and assess opportunities to reduce water demand.

Beyond general obligations and policy statements published by individual States, Territories and water authorities, there are currently no binding efficiency, sustainability or social impact laws, regulations or guidelines for the procurement or use of water specifically relating to data centres.

As outlined in the 'Power' section above, the Expectations state that data centre developers should prioritise sustainable and efficient water usage, for example, by using non-potable water where possible.

In March 2026, the NSW Government published the NSW Data Centre Consultation Paper for feedback. The Consultation Paper sets out a range of proposed key principles for data centre investment and regulation, including that data centres 'make sustainable use of our energy and water systems'. Similar to the Commonwealth Government's list of expectations above, it emphasises that data centres should use recycled water for water-intensive cooling systems where feasible.

There is also potential for future regulatory reform regarding water supply for data centres across Australia, including where water regulation is a key focus for the current Parliamentary Inquiry into data centres in NSW and proposed national AI Standards (see 'Power' section above for further details).

03 Land

What approvals and permits are required?

The development, construction and operation of data centres will typically require several permits and land related approvals, which vary by state and local jurisdiction.

- Planning approvals require a development application, submitted to local council or state planning authority and relating to appropriately zoned land.
- Building permits are required before construction begins to ensure the design complies with building codes and regulations.
- Approvals from utility providers, in particular electricity, water and telecommunications, may also be necessary
- Federal environmental approvals may be required where data centre projects have potential significant impact on a 'matter of national environmental significance' (eg threatened flora and fauna).

Several States and Territories also have fast-track mechanisms for data centre-related planning approvals, such as the Development Facilitation Program (**DFP**) in Victoria. The DFP enables streamlined planning approvals for data centre projects with a development cost of over A$20 million (in metropolitan Melbourne) or A$10 million (in regional Victoria). For example, in February 2026, a A$1 billion data centre project in Port Melbourne was approved under the DFP within only 75 days of the original planning application being lodged.

Victoria's Sustainable Data Centre Action Plan, released in September, seeks to attract investment while imposing clearer requirements for new projects, including limits on location, a 150-metre buffer from homes, non-drinking water for cooling and local community benefits.

How long does permission take?

The timeline for securing these permits and approvals can vary, but usually ranges from a few months to several years, depending on, various factors, including the complexity of the project, and the processes of the local and state planning authorities.

Where can you build and what if rezoning is needed?

Zoning regulations are established by local and state planning authorities and vary between states and local regions. Typically, data centres can be developed and used on land in industrial or special purpose zones related to technology or data centre use.

Data centre developers should engage with the relevant planning authority to ensure land is appropriately zoned.

Land can be re-zoned, but this usually requires an environmental assessment, as well as a community consultation process. The prospects of re-zoning and the time required to secure approval will be affected by environmental considerations, the surrounding locality and consistency with strategic plans and policies for the relevant area.

Australian Government Expectations

Government agencies will likely prioritise proposals that most closely align with the Expectations. New planning approval processes, though they may not create strict regulatory obligations, will likely take into account a range of 'social licence' factors that may influence project feasibility.

The Australian Government has indicated its intention to embed the Expectations into approval and planning processes across the States and Territories. This has already commenced in NSW, with the government announcing consultation for a move to principles-based regulation over data centre investment.

New South Wales new planning body and inquiry

In 2025, the NSW Government established the Investment Delivery Authority (**IDA**) to accelerate the approval of major projects across all industries, including data centres. The first round of expressions of interest opened in late 2025.

In March 2026, the Government announced that the IDA would support 15 new data centre projects valued at A$51.9 billion, adding to the 90 data centres already operating in NSW. Several of the new centres will be located in Western Sydney suburbs including Blacktown, Fairfield, and Penrith.

Further policy developments can be expected in late 2026 after the end of the consultation period for the NSW Data Centre Consultation Paper which was released in March.

An inquiry into the development and regulation of data centres across NSW was also established on 29 January 2026, with a final report from the NSW Legislative Council Public Accountability and Works Committee due by 30 September 2026.

Victoria fast-tracking planning applications

With 40 existing data centres, Victoria holds about one-third of the A$30 billion market for data centres in Australia, compared with NSW which holds about 56%. With the release of the Sustainable Data Centre Action Plan in February 2026, Victoria is seeking to become a leader in data centre investment.

In 2024, it established the Development Facilitation Program (**DFP**) to provide for expedited planning pathways for priority projects including data centre projects.

In the past few years, the Victorian Government has fast tracked the planning applications for several major data centre projects (with an approval timeframe as short as 28 days in some instances).

Federal environmental streamlining reform

Data centre projects with potential to have a significant impact on 'matter of national environmental significance' may require referral, assessment, and/or approval by the Federal Minister under the *Environment Protection and Biodiversity Conservation Act 1999* (Cth), which can extend approval timeframes.

However, there are 'streamlining reforms' commencing later in 2026 which could assist data centre development, by providing a pathway for projects with detailed, upfront assessment information that are able to comply with National Environmental Standards.

04 Telecommunications

Industry assistance

Part 15 of the *Telecommunications Act 1997* (Cth) empowers law enforcement or national security agencies to request assistance from 'designated communications providers' (**DCPs**) in relation to national security or law enforcement matters.

Data centre operators may be considered DCPs, for example, if they are providing electronic services such as cloud service add-ons, telecommunications links or internet connectivity as part of an internet exchange operation or other bundled service, or services that facilitate, or are incidental to, carriage or electronic services.

Law enforcement or national security agencies may issue notices to DCPs requesting that they perform certain activities or develop new capabilities to assist with investigations. Notices are generally either:

- mandatory (technical assistance notices and technical capabilities notices), or
- voluntary (technical assistance requests).

The activities that can be requested of DCPs who are data centres include:

- providing technical information relating to the data centre facilities such as design, manufacture information
- installing, maintaining or testing software at the data centre
- giving information to or assisting law enforcement under a warrant or authorisation to carry out a warrant
- providing access to software used in connection with electronic services, or facilities at its data centres, or
- concealing covert actions by law enforcement at its data centre.

Technical assistance cannot be requested by agencies to introduce a systematic weakness or vulnerability, to inadvertently weaken the information security or compel a provider to build a decryption capability or make their encrypted systems less effective.

Is a telecommunications licence required?

A carrier licence is not generally required to operate a data centre.

However, a carrier licence may be required to own certain telecommunications infrastructure associated with a data centre, such as dark fibre. Certain VAS supplied with a data centre service, such as an internet connectivity service, may also bring an operator in scope as a carriage service provider.

05 Foreign investment restrictions

Certain investments by a 'foreign person' cannot proceed without a 'no objection notification' from the Australian Treasurer under the *Foreign Acquisitions and Takeovers Act 1975* (Cth) (**FATA**), which governs foreign investment in Australia (commonly known as **FIRB Approval**).

A 'foreign person', for entities, is either:

- a single investor from a foreign country holding at least 20% interest in the entity, or
- two or more investors from any foreign country holding in aggregate at least 40% interest in the entity (disregarding foreign holdings that are less than 5% for entities listed primarily on the Australian stock exchange).

Whether an investment requires FIRB Approval depends on various factors. This may include whether the foreign person is a foreign government investor (**FGI**) (which can include companies with less-than-majority stakes ultimately held by a foreign government), its jurisdiction of incorporation, and the characterisation of the proposed target under the FATA.

If a proposal requires FIRB Approval, the Australian Treasurer will consider whether it is contrary to the national interest, as the legal test under the FATA. This broad national interest assessment could include:

- national security
- digital sovereignty
- community concerns, and
- how well the proposal aligns with the Australian Government's Expectations for data centres.

Want a 'playbook' to work out – and improve - the prospects for a foreign bid?

Read our guide, Conditionally yours: Tackling FIRB uncertainty in foreign bids

Land requires FIRB approval

The acquisition of an interest in land by a foreign person, unless below a monetary threshold, requires FIRB approval.

Data centres as 'critical infrastructure'

The FATA captures certain investments by foreign persons relating to critical infrastructure assets under the SOCI Act. This may include data centres that are critical data storage or processing assets. Businesses that are a responsible entity or direct interest holder in respect of critical infrastructure assets are 'national security businesses'.

These investments are generally 'notifiable national security actions', and the Treasurer will need to be satisfied that the foreign person's proposed investment is not contrary to Australia's national interest and national security before issuing a FIRB approval.

Commonly, FIRB approval is required for:

- the acquisition of at least 10% interest or any control or influence by a foreign person in a data centre business that is a national security business, regardless of business value, and
- the starting of a new data centre business, that is a national security business, by a foreign person, regardless of business value.

Other restrictions

Even if a data centre is not considered a critical infrastructure asset under the SOCI Act, there are other general percentage and monetary thresholds that apply to foreign investments that may require FIRB approval. For example, the acquisition of an at least 20% interest by a foreign person in an Australian business or entity that exceeds the relevant monetary threshold.

You can check the current monetary thresholds on the government's Foreign investment in Australia page.

Proposed foreign investment regime reforms

In May 2026, the Australian Government announced proposed reforms to streamline low-risk foreign investment while strengthening the regime's response to sensitive investments, national security risks, non-compliance and avoidance. The timing and operation of many measures remain subject to further development and consultation.

- **Proposed streamlining measures:** removing approval requirements for some minor or incremental acquisitions, raising the A$347 million threshold for certain non-sensitive investments and targeting 30-day decisions for qualifying low-risk applications from 1 January 2027.
- **Proposed strengthening measures:** broader powers to impose conditions and intervene in sensitive investments, stronger enforcement, and scrutiny of commercial arrangements such as lending and offtake that may confer influence or control.

For data centre transactions, this may require closer assessment of financing, governance, customer and other contractual arrangements - not only equity ownership.

Foreign investors should map regulatory risk across the complete investment structure, including equity, debt, governance rights, long-term capacity or commercial arrangements, ownership changes and post-completion obligations. Project timetables should allow sufficient time as data centre proposals are most likely to be sensitive.

06 Tax and other incentives

Special economic zones

None.

Tax incentives

If a managed investment trust **(MIT**) invests in a data centre that obtains a 6-star rating from Green Building Council Australia or a 6-star NABERS rating, the MIT can access a concessional 10% withholding tax rate on fund payments to foreign investors. Introduced from 1 July 2025, this concession only applies where construction of the data centre commenced after 9 May 2023.

Other incentives

None.

ON THE GROUND

Investing (in regional) Down Under

As demand grows, we may see a trend toward the development of data centres in less traditional locations, including in regional areas. This may help alleviate some of the constraints posed by limited urban land availability and provide opportunities for lower operational costs.

Limited stock is also driving the trend for leasing and other strategic partnerships as a means for hyperscalers (who previously may have been owner/builders) to secure competitive space for data centres in the Australian market.

07 Data protection and cyber security

Data protection or privacy laws

The Australian Privacy Principles (**APP**) are the cornerstone of data protection and privacy in Australia contained in Schedule 1 of the *Privacy Act 1988* (Cth) (**Privacy Act**). An organisation or business covered by the rules - an 'APP entity' - must take reasonable steps to protect personal information it holds from misuse, interference and loss, as well as unauthorised access, modification or disclosure.

Reasonable steps will depend on specific circumstances such as the nature of the entity (size, resources) and the amount and sensitivity of the personal information held.

This requirement does not apply to data centre operators in relation to personal information held by data centre customers on their own IT equipment within a data centre (such as a colocation arrangement). In that scenario, it would only apply, in relation to personal information that the data centre itself holds (for example, about customer personnel). However, a hosting service provider may have obligations under the Privacy Act and SOCI Act (see 'Critical infrastructure and security' section below for further details), in relation to the data it hosts.

Most businesses are caught by these rules. 'APP entity' means an agency or organisation except a small business operator, registered political party, State or Territory authority. In general, a small business operator has an annual turnover of AU$3 million or less in a financial year, unless an exception applies (for example, the business provides a health service or is a contracted service provider for a Commonwealth contract).

Beyond these general APPs, there are no direct data protection or privacy laws specifically for data centres.

Copyright a bottleneck for AI investment?

Governments, courts and rights holders around the world continue to consider copyright licensing and AI training frameworks. In Australia, proposed AI standards would include conditions intended to support the local creative, cultural and media sectors.

Broader uncertainty over copyright licensing for AI training remains and may constrain investment and deployment.

Read more: Australia's next AI bottleneck: Why copyright matters.

Cyber security laws

Responsible entities of data centres classified as critical infrastructure (see 'Critical infrastructure and security' section below for further details), must notify the Australian Cyber Security Centre of:

- cyber security incidents that have a significant impact (direct or indirect) on the availability of its 'critical data storage or processing assets', which are a type of 'critical infrastructure assets' captured by the SOCI Act (see 'Critical infrastructure and security' section below for further details) - notification is required within 12 hours of becoming aware of the incident, under the SOCI Act, and
- other cyber security incidents that have an impact on the availability, integrity or reliability of its critical data storage or processing assets, or on the confidentiality of information about its asset or stored in the assets, within 72 hours of becoming aware of the incident.

The Minister of Home Affairs may also optionally declare critical infrastructure assets to be 'systems of national significance'. As a result, they are then subject to enhanced cyber security obligations, including:

- developing cyber security incident response plans
- undertaking cyber security exercises
- undertaking vulnerability assessments, and
- providing reports about system information.

08 Critical infrastructure and security

Critical infrastructure laws

The SOCI Act regulates the operations of certain infrastructure assets and services that the Australian government considers to be of critical importance to the national interest (including the economy, the functioning of government and public wellbeing), including data centres.

Responsible entities (owners or operators of data centres) must comply with additional compliance obligations if their facility is a 'critical data storage or processing asset' (a type of 'critical infrastructure asset') under the SOCI Act. These obligations include:

- registering the data centre with the regulator (the Cyber and Infrastructure Security Centre), which requires:
  - responsible entities to provide the regulator operational information about the entity and the facility, and
  - direct interest holders in the facility to disclose interest and control information in relation to the entity and the asset
- except where the data centre has a HCF Strategic certification, the responsible entity implementing and maintaining a critical infrastructure risk management program (**CIRMP**), to identify hazards (including physical security and natural hazards), and put in place measures to minimise or prevent them
- the responsible entity reporting cyber security incidents to the regulator, within very short timeframes (see 'Data protection and cyber security' above for further details), and
- complying with government directions following incidents impacting the data centre.

Data centres will be considered a 'critical data storage or processing asset' under the SOCI Act if:

- the asset is used wholly or primarily to provide data storage or processing services that relate to business critical data and is provided to an end user that is either:
  - the Commonwealth, a State or a Territory, or a body corporate established by a law of the Commonwealth, a State or a Territory, or
  - the responsible entity of a critical infrastructure asset, and
- the entity that owns or operates the data centre knows that the asset is being used in this way.

'Business Critical Data' means:

- personal information (within the meaning of the Privacy Act) that relates to at least 20,000 individuals
- information relating to any research and development in relation to a critical infrastructure asset
- information relating to any systems needed to operate a critical infrastructure asset
- information needed to operate a critical infrastructure asset, or
- information relating to risk management and business continuity (however described) in relation to a critical infrastructure asset.

Proposed SOCI reforms

An Independent Review into the SOCI Act, delivered on 2 February 2026, recommended a suite of reforms. Following that review, the government made Enhanced CIRMP Rules on 10 June 2026 that impose additional risk management obligation on responsible entities for certain asset classes (although not data centres).

On 3 July 2026, the government released a consultation paper proposing further reforms to streamline and modernise the SOCI Act, which if implemented, would increase the number of asset classes that will be regulated by the SOCI Act and increase the government's powers to direct compliance with, and to enforce, the SOCI Act.

It will therefore be important for operators and investors of critical infrastructure assets to stay on top of their SOCI Act obligations.

Relevantly, the government proposes to replace the current approach for capturing data centres as critical infrastructure assets under the SOCI Act. Under the proposed model, data centres will be captured through four alternative pathways:

- **facility-based capture:** based on physical and operational characteristics, principally rated IT load, with a proposed starting point of 1MW
- **service-based capture:** based on type and scale of service as is the case with the existing data storage or processing test, but with thresholds set by reference to matters such as Australian revenue, customer numbers, data volume or employee headcount
- **certification-based capture:** based on certification held by the provider, for example under the HCF certification scheme, and
- **reserve Ministerial designation:** for exceptional cases of government dependency.

Operators should assess whether their facilities could be captured under the proposed pathways and review their SOCI Act obligations, including CIRMP governance, operational control and critical supplier arrangements.

National security issues

There are various national security considerations for data centres in Australia.

Under the Commonwealth Government's Protective Security Policy Framework (**PSPF**), Commonwealth government entities can only procure hosting services from providers that have obtained HCF Strategic certification, which extends to cloud services and the infrastructure underpinning those cloud services.

However, the HCF certification scheme is currently undergoing reform as part of the Australian government's broader cyber security strategy. When the reforms are finalised, both new service providers seeking certification and existing certified service providers will be required to comply with the reformed HCF framework if they want to supply services to the Australian government.

Data centre operators should keep up to date with relevant developments on the HCF framework and how it may impact their business, to ensure that the regulated entity's information assets are stored securely.

Prospective responsible entities, or direct interest holders, of data centres that meet the threshold of a 'critical data storage or processing asset' are considered 'national security businesses' under the FATA, and acquirers will need to obtain FIRB approval before acquiring these assets given the A$0 FIRB threshold for national security businesses.

FIRB approval will only be granted for those assets if the Treasurer is satisfied that a foreign person's proposed investment is not contrary to Australia's national interest and national security (see 'Foreign investment restrictions' above for further details).

Data centre operators may be required under various Federal, State and Territory laws to comply with surveillance warrants, emergency authorisations, assistance orders, or search and seizure warrants obtained by law enforcement officers or security agencies.

Data centre operators may also receive notices to produce from federal or state police, requiring the disclosure of documents and information relevant to investigations into serious terrorism and other offences (such as those punishable by 2 or more years' imprisonment).

Defence export controls

Defence Trade Controls Act 2012 (Cth)

The *Defence Trade Controls Act 2012* (Cth) (**DTC Act**) regulates the export and supply of goods and technologies listed on the *Defence and Strategic Goods List 2021* (Cth) (**DSGL**). Importantly, the export control regime extends:

- beyond physical exports to capture supplies to 'foreign persons' within Australia, and
- to the provision of remote access to controlled technology.

Determination of whether goods or technology are included on the DSGL begins with a technical classification exercise. Certain data centre technology (for example, certain cloud infrastructure or high-performance computing equipment) may, depending on the scope of the operator's activities, meet specified criteria of items within the DSGL's Dual-Use List.

The application of the DSGL will also be informed by whether the technology is required for the 'development', 'production' or 'use' of controlled goods.

If a data centre's activities involve the supply of DSGL technology, any access to DSGL technology provided to a foreign person (for example, customers or the data centre's own employees), regardless of location, may require a permit from Defence Export Controls unless an exemption or exception applies.

There are various exemptions and exceptions available, for example under the DTC Act there is a 'licence-free' environment for certain exports between Australia, the United Kingdom and the United States. Non-compliance with the DTC Act carries significant penalties, including fines or potential imprisonment.

In practical terms, data centre operators should assess:

- whether any of its goods, software or technology are listed on the DSGL
- whether the supply of those items to any third party requires a permit (which requires an assessment of whether any exemptions or exceptions apply)
- whether the supply of those items to any employee requires a permit (which also requires an assessment of whether any exemptions or exceptions apply)
- if yes to the second and third points above, whether the target or operator holds or requires permits from Defence Export Controls for the relevant supplies, and
- whether any internal compliance systems are in place to identify and manage regulated supplies.

Weapons of Mass Destruction (Prevention of Proliferation) Act 1995 (Cth)

Given the nature of computing technology for data centres, consideration needs to be given to the *Weapons of Mass Destruction (Prevention of Proliferation) Act 1995* (Cth).

At a high level, this Act prohibits the supply of services or the export of 'non-regulated' goods (being goods not otherwise prohibited under the *Customs Act 1901* (Cth)) where the provider or exporter believes or suspects, that the services or goods will or may be used to assist a weapons of mass destruction program, unless authorised by a permit.

Physical security issues

To obtain HCF Strategic certification, data centre providers must demonstrate that their data centre, or a separate enclave within their facility, is constructed to the appropriate zone specifications set out in the PSPF. HCF Strategic certification is generally a prerequisite for providing services to Australian government customers or supporting those who do.

These security requirements have been determined by the Security Construction and Equipment Committee (**SCEC**), an Australian government body that evaluates security equipment for use by government agencies.

As part of the HCF application, the SCEC may evaluate a data centre's compliance with the zone specifications.

Financial services providers or financial institutions

In Australia, financial services providers and financial institutions must comply with requirements relating to operational risk and the management of data and information security, including the Australian Prudential Regulation Authority (**APRA**) Prudential Standards such as CPS 230 and CPS 234.

These requirements will apply to data centre operators:

- directly if they themselves are regulated entities, or
- indirectly if their client is a regulated entity.

Where regulated entities outsource their functions (such as data storage), they are responsible for ensuring that their service providers meet the relevant standards (or at least, to perform the relevant services in a manner that allows the regulated entity to meet the relevant standards).

Of particular relevance to data centre operators is an obligation on prudentially regulated entities to ensure that its outsourced service providers allow the entity, or APRA, to conduct on-site audits of the service provider's facilities to ensure that the regulated entity's information assets are stored securely.

09 Data localisation

Highly regulated sectors and health information

Data centres that hold health information on Australians must not:

- hold or take those records outside Australia
- process or handle information relating to those records outside Australia, or
- cause or permit another person to do either under the *My Health Records Act 2012* (Cth).

Privacy laws

Generally, data centre operators and customers who are subject to the APPs (see 'Data protection and cyber security' above for further details) cannot disclose personal information to an overseas recipient before taking reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the information.

The disclosing entity is responsible for the acts or practices of the overseas recipient, unless:

- the disclosing entity reasonably believes the overseas recipient is subject to a law or binding scheme that has a substantially similar effect of protecting information as the APPs, or
- the entity has obtained the individual's consent, where expressly informed the APPs will not apply to overseas disclosure.

Commonwealth, state and territory government data

There are no explicit data offshoring restrictions on government data in legislation. However, Commonwealth and state governments will often have policies restricting data offshoring, or at least an implicit preference for their data to be stored in Australia.

For example, the Western Australian government has a data offshoring policy that requires 'Tier 1' category data, which is certain categories of 'Official Sensitive' data and digital identity data, to be hosted in Australia.

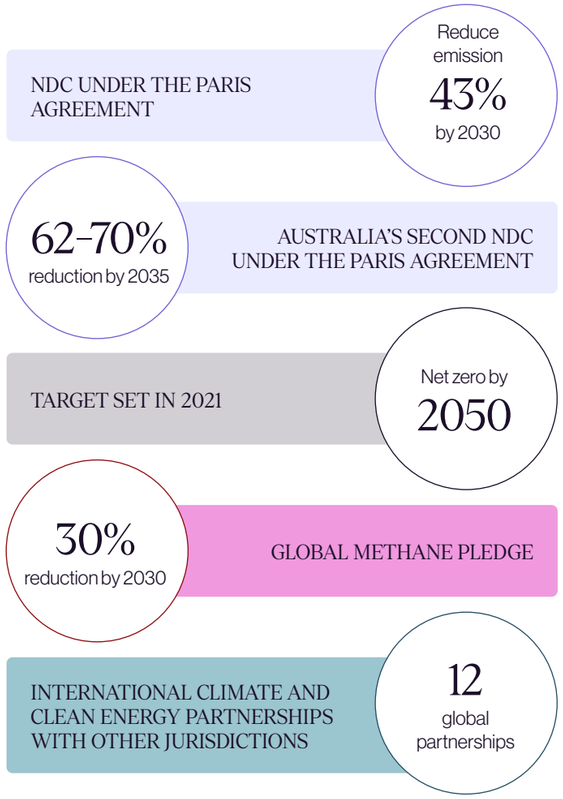
Additionally, the HCF requires federal government's ability to procure data centre services from certified data centres, which are all located in Australia.

Accredited service providers to the 'Gatekeeper Public Key Infrastructure Network' are also required to be physically located within Australia and provide services from Australia. Accordingly, most government data is, in practice, hosted in Australia.

10 Environmental, social and governance

International ESG commitments

Australia is a signatory to the Paris Agreement and in September 2025, the Australian government submitted Australia's second Nationally Determined Contribution (**NDC**) detailing Australia's 2035 targets. The *Climate Change Act 2022* (Cth) and *Climate Change (Consequential Amendments) Act 2022* (Cth) (**Climate Acts**) formalised Australia's international obligations.



ESG laws, regulations and guidelines

There are no specific efficiency, sustainability or social impact laws relating to data centres in Australia. However, as mentioned above, only data centres with a 5-star NABERS rating can secure government work.

ESG reporting

A climate financial disclosure regime requires certain organisations to disclose climate related risk and opportunities that could reasonably affect their cash flow, access to finance or cost of capital. This is under the *Treasury Laws Amendment (Financial Market Infrastructure and Other Measures) Act 2024* (Cth) (**Climate Disclosure Regime**).

The Climate Disclosure Regime groups organisations into three tiers - of which data centres are likely to fall within one - that determine when the obligations start.

Largest entities (Group 1)

From 1 July 2026, entities must report if they meet at least two of the following:

- consolidated revenue of A$500 million or more
- consolidated gross assets of A$1 billion or more at the end of the financial year (**EOFY**), or
- Full-time equivalent (**FTE**) employees of 500 or more at EOFY.

Alternatively, the Group 1 reporting obligations are also applied to entities that are National Greenhouse Energy Reporting Scheme reporters which the Clean Energy Regulator publishes emissions data about.

Second largest entities and asset owners (Group 2)

From 1 July 2026, entities must report if they meet at least two of the following:

- consolidated revenue of A$200 million or more
- EOFY consolidated gross assets of A$500 million or more, or
- EOFY FTE employees of 250 or more.

Alternatively, the Group 2 reporting requirements also apply to entities registered or required to be registered under the *National Greenhouse and Energy Reporting Act 2007* (Cth) or are asset owners with assets at the end of the financial year valued at equal to or greater than AU$5 billion.

All other in-scope entities (Group 3)

From 1 July 2027, entities must report if they meet at least two of the following:

- consolidated revenue of A$50 million or more
- EOFY consolidated gross assets of A$25 million or more, or
- EOFY FTE employees of 100 or more.

Contributors



Daryl Cox

PARTNER
SINGAPORE

TEL +65 87253595
MOB +65 6991 6506
EMAIL daryl.cox@mallesons.com



Aaron Ong

SENIOR ASSOCIATE
SINGAPORE

TEL +65 6991 6524
MOB +65 8226 3417
EMAIL aaron.ong@mallesons.com



Daniel Chan

SENIOR ASSOCIATE
SINGAPORE

TEL +65 6991 6515
EMAIL daniel.chan@mallesons.com



Charles Davies

SENIOR ASSOCIATE
SYDNEY

TEL +61 2 9296 2257
MOB +61 428 918 076
EMAIL charles.davies@mallesons.com



Wesley Yu

ASSOCIATE
SINGAPORE

TEL +65 6991 6559
MOB +61 477 902 714
EMAIL wesley.yu@mallesons.com



Thalia Velez Rodriguez

SOLICITOR
MELBOURNE

TEL +61 3 9643 4233
MOB +61 456 551 089
EMAIL thalia.velezrodriguez@mallesons.com



Samantha Gates

SOLICITOR
MELBOURNE

TEL +61 3 9643 5351
MOB +61 4 6125 5836
EMAIL samantha.gates@mallesons.com



Charlotte Hartley

SOLICITOR
MELBOURNE

TEL +61 3 9643 4450
MOB +61 461 405 237
EMAIL charlotte.hartley@mallesons.com



Gary Smythe

HEAD OF MARKETING – CONTENT & CAMPAIGNS
MELBOURNE

TEL +61 3 9643 5351
MOB +61 408 064 429
EMAIL gary.smythe@mallesons.com



Katie Walsh

CONTENT & CAMPAIGNS LEAD
SYDNEY

TEL +61 2 9296 3275
MOB +61 431 759 334
EMAIL katie.walsh@mallesons.com

We are grateful for those who have shared their insights from across APAC and helped to bring this Guide to life, from Mallesons and beyond.

We have strong, established relationships with leading law firms from around the Asia region, who we worked with to bring this together. A special thank you to ABNR, Chandler Mori Hamada, Chapman Tripp, Frasers Law Company, Kim & Chang, King & Wood, Lee and Li, Mori Hamada, Romulo Mabanta Buenaventura Sayoc & de los Angeles, Skrine and Trilegal for their collaboration on this Guide.

Australia

Mallesons
Intan Eow
Francesca Giorlando
Emily Heffernan
Lizzie Knight
Cheng Lim
Cate Nagy
Greg Protektor
Roderick Smythe
Josh Thorneycroft
Chris Wright
Jayson Broadway
Esther Yee
Anthea Shan
Jonathan Beh

China

King & Wood
Susan Ning
Han Wu

Hong Kong SAR

King & Wood
Tian Xu
Scott Gardiner
Vince Lee
Francois Tung

India

Trilegal
Jishnu Sanyal
Janak Pradhan
Samsuddha Majumder
Amar Narula
Kartikey Kulshrestha
Kuruvila M Jacob
Atyotma Gupta
Archita Sharma
Adi Kidambi
Ojas Date

Indonesia

ABNR
Ayik Candrawulan Gunadi
Agus Ahadi Deradjat
Mohammad Afif Hirzi
Edmund Khovey
Beverly Sharon Laza
Emir Nurmansyah
Nina Cornelia Santoso
Adya Sepasthika
Mahiswara Timur

Japan

Mori Hamada & Matsumoto
Satoru Hasumoto

Malaysia

Skrine
Tan Wei Xian
Belinda Lim Ke Xin
Fariz Bin Abdul Aziz
Cheam Tat Sean
Rachel Chiah
Natalie Lim
Siti Ayeena Binti Mohd Anis
Jesy Ooi
Engy Tan Shin Chian
Kyra Iman Yaacob

New Zealand

Chapman Tripp
Kelly McFadzien
Lauren Curtayne
Hamish Bolland
Alana Lampitt
Tessa Baker
Bevan Miles
Guy Houghton-Jones
Max Williams
Conor Tinker
Tamsin Gorman
Hannah Houghton

Philippines

Romulo Mabanta Buenaventura Sayoc & de los Angeles
Peter Pacheco
Agustin R Montilla IV
Rafael D del Rosario
Jesse Eleazer D Tantoco

Singapore

Mallesons
Daryl Cox
Daniel Chan
Wesley Yu
Aaron Ong
Charlotte Handley

South Korea

Kim & Chang
Kye Sung Chung
Jin Ho Song
Arnold Yoo-Hum Baek
Yu Seok Jung
Sang Hoon Richard Sung
Seung Hoon Yeom

Taiwan

Lee and Li
Lily Kuo
Sarah Wu
Chi Lee
Helen Huang

Thailand

Chandler Mori Hamada
Jessada Sawatdipong
Panupan Udomsuvannakul
Sarunporn Chaianant
Koraphot Jirachocksubsin
Suphakorn Chueabunchai
Thanachart Osathanondh

Vietnam

Frasers Law Company
Ho Thuy Ngoc Tram
Mark Fraser
Hoang Thi Thuy Vy
Tran Le Minh Truc

Many people contributed to the development of this Guide and we greatly appreciate their assistance.

Kristen Dwyer
Chelsie Easton
Emily Fox
Hannah McNab
Siddhi Pulekar
Hamish Nicholson
James Walker
Nadia Wust
Abraham Alvarez (TAG design)
Damien Winddow (TAG design)
DC Byte.

About Mallesons

We are Mallesons. The top-tier independent firm from Australia, a full-service firm trusted on the most complex and consequential matters across our region and around the world.

Our independence gives us the flexibility to combine our top tier full-service capability with the best advisers in every market.

We have 200 partners and over 1,500 lawyers who are locally qualified and globally experienced.

We're here to be the firm clients and communities trust most with their future in a world that never stands still. To have an outsized impact. To lead the market. To make a difference to be proud of. To create careers that can go everywhere.

Click here to access our full Data Centre APAC Regulatory Guide covering all 14 markets and exploring key themes across the region.

Join the conversation

mallesons.com

Disclaimer
This publication is prepared by Mallesons for general information only. It does not constitute legal or other professional advice. You should seek specific legal advice from a Mallesons legal professional before acting on any information contained in this publication.