



K W M D I G I T A L E C O N O M Y

DATA CENTRES

APAC REGULATORY GUIDE

JULY 2025

KING&WOOD
MALLESONS
金杜律师事务所

Wisdom by Basia Nowacki

THE DIGITAL REVOLUTION IS BRINGING OPPORTUNITIES

Over the last decade, data centres have emerged as one of the most significant asset classes for investment globally. Funds initially followed the growing demand for cloud technologies, as enterprises moved away from on-premises processing. More recently, the accelerated build-out of infrastructure to support the world’s appetite for AI has emerged as another key driver.

Harnessing these opportunities without 'hype-crash' risk requires sectoral intelligence.

The APAC region has experienced a significant portion of data centre growth in a trend that is set to accelerate. The region is expected to require 1.7 times the capital of the US to develop its pipeline. Local development opportunities are evolving, as cloud service providers and enterprises increasingly build capacity in-country instead of operating from regional gateways. This is creating opportunities for investors to build and operate data centres in jurisdictions with traditionally low capacity.

Yet regulatory requirements across the APAC region vary and can be opaque. In some cases, there is a perception of having to take ‘sovereign risk’ when investing in emerging economies.

This Guide shares the 8 key themes you need to know about the APAC market. In addition, it contains a 'regulatory heatmap' and detailed jurisdictional snapshots for 13 key markets.

For a deeper dive into any of these key markets, contact one of our experts. We can provide tailored advice on how to navigate the regulatory challenges.

60%

of the world's population resides in the APAC region, where economies are rapidly growing, modernising and digitalising.

WHAT YOU'LL FIND IN THIS GUIDE

The regulatory landscape - laws, policies, market practices - relating to:



Power and water sourcing



Land acquisition and use



Telecommunications



Foreign investment controls



Tax and other incentives



Critical infrastructure and security



Data protection and data localisation



ESG



Sector-specific regulations

‘Understanding the diverse markets of the APAC region - at a deep, local level - is critical for participating in the phenomenal data centre growth story that is unfolding. This Guide is designed to help. We're thrilled colleagues from 13 key markets could join us to bring these insights to you.’

Daryl Cox



Daryl Cox

Partner, KWM



Ursula McCormack

Partner, KWM



Cheng Lim

Partner, KWM

DATA CENTRES - APAC REGULATORY GUIDE 2025

2

3



CONTENTS

4

Key regulatory themes to navigate

18

A regional snapshot

20

Australia | Chapter 1

32

China | Chapter 2

42

Hong Kong SAR | Chapter 3

52

India | Chapter 4
Support from Trilegal

62

Indonesia | Chapter 5
Support from ABNR

72

Japan | Chapter 6

80

Malaysia | Chapter 7
Support from Skrine

90

Philippines | Chapter 8
Support from Romulo Mabanta Buenaventura Sayoc & De los Angeles

98

Singapore | Chapter 9

106

South Korea | Chapter 10
Support from Kim & Chang

118

Taiwan | Chapter 11
Support from Tsar & Tsai Law Firm

128

Thailand | Chapter 12
Support from Chandler Mori Hamada

136

Vietnam | Chapter 13
Support from Frasers Law Company

150

Glossary

SOME TERMS UNCLEAR?

CHECK OUT OUR GLOSSARY, WHERE WE EXPLAIN VARIOUS TERMS USED THROUGHOUT THIS GUIDE.



KEY REGULATORY THEMES TO NAVIGATE

From power availability to AI sovereignty, this Guide highlights several important regulatory trends for data centres. Mapping and navigating them is essential for sustainable investments and operations in each market.

For further detail on the themes in each market, please see the local jurisdictional snapshots.

8 REGULATORY THEMES TO WATCH



1. POWER



2. GOING GREEN



3. WATER



4. GOVERNMENT INCENTIVES



5. UNLOCKING FOREIGN INVESTMENT CONTROLS



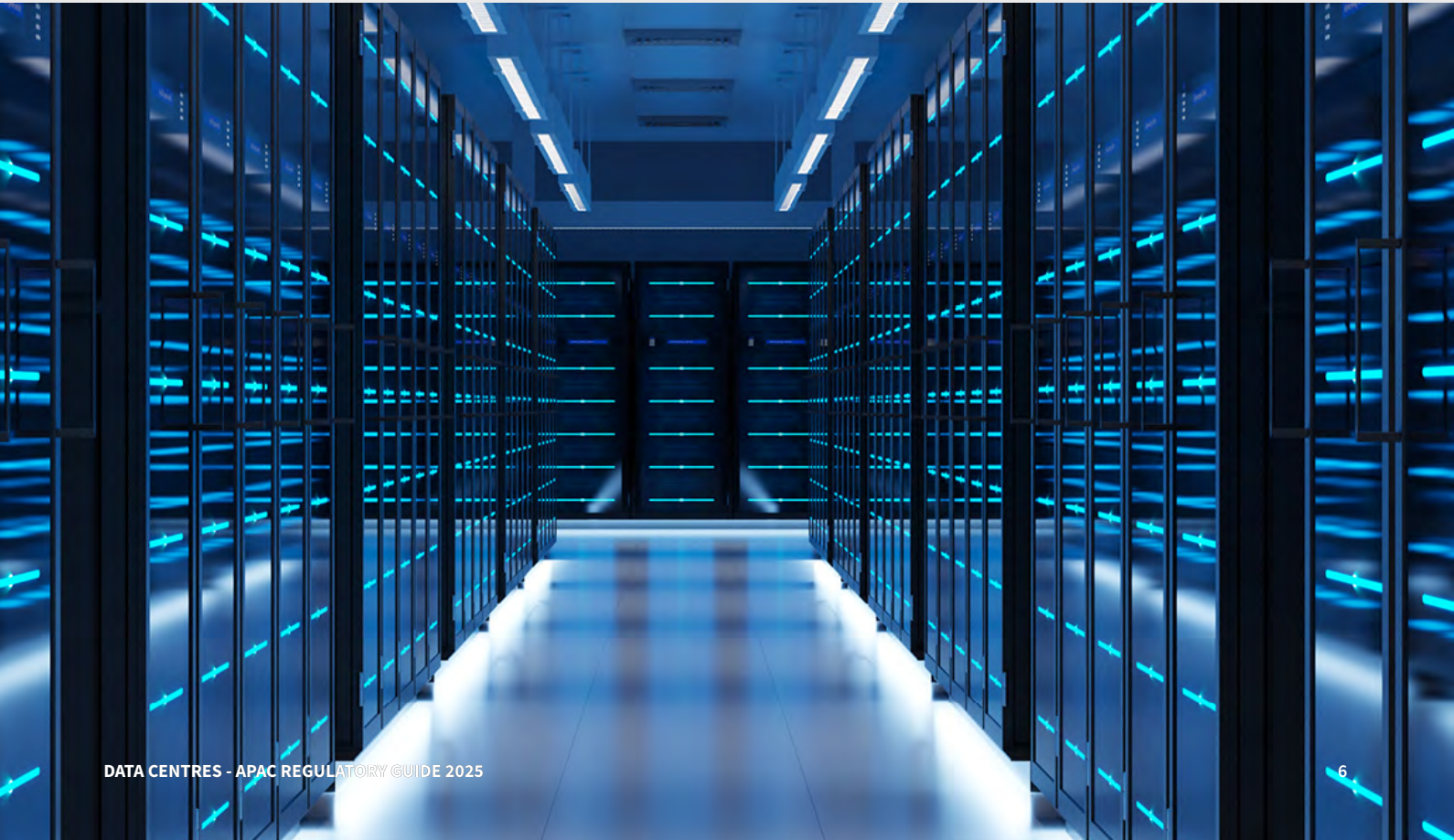
6. LOCAL DEMAND V DATA LOCALISATION



7. INFLUENCE OF EXPORT CONTROLS



8. NATIONAL SECURITY & AI SOVEREIGNTY



THEME 1

Data centres require more power and its availability is a critical enabler across all markets

The availability of stable and reliable power is a decisive factor for selecting data centre sites across APAC. As data centres scale up to meet the demands of cloud computing and generative AI, power requirements have increased, making energy availability a major bottleneck across all markets.

The power challenge persists

Even before recent data centre growth, many jurisdictions encountered issues with the stability and availability of their electricity grid.

Governments in all jurisdictions are now having to balance market demand for more data centres (and their associated power load) with competing objectives, such as electrification of daily activities and decarbonisation of the energy industry.

Governments are responding (but approval and connection times are still long)

In both developed and developing markets across the region, government or grid operator approvals for data centre projects focus on the existing grid to service new data centres. Many jurisdictions have a requirement to undertake a power impact assessment before a connection request is granted. This can increase lead times for approvals and, from a developer's perspective, complicates the site selection and acquisition process.

Fast approvals and innovative approaches are appearing

Depending on the location, sites in emerging jurisdictions such as India, Vietnam and Indonesia may get approved faster, in some cases within a few months. However, timelines will vary from location to location within each jurisdiction based on the extent of power distribution infrastructure available.

With these constraints, some governments are encouraging the development of new data centres away from populated areas and closer to power generation.

For example, **Japan's** Ministry of Economy, Trade and Industry offers financial incentives to develop facilities away from Tokyo and Osaka.

In **South Korea**, there is increasing pressure to move data centre capacity closer to the generation on the East coast (where the bulk of the nuclear generation capacity is located).



ON THE GROUND

LOCAL POWER CHALLENGES

Japan

Securing an electricity connection from TEPCO (local grid utility) near Tokyo can take over 10 years due to limits on existing grid capacity and the difficulties in expanding it to meet current levels of demand.

South Korea

KEPCO's lead time for new connections is between 1 to 4 years for data centres of any significant size. Anecdotally, it is difficult to secure approval for new power connections to data centre sites in or near Seoul.

Singapore

Lead times for new connections are typically over 2 years, with the more fundamental constraint of having to secure access to data centre capacity through government-managed Data Centre Call for Application (**DC-CFA**) processes after the 3-year moratorium on new developments was lifted in 2022.

Australia

Lead times are often more than a year. A moratorium on new data centres in selected regions, for example the Macquarie Park data centre hub near Sydney, was announced in May 2025.



Assess power sources for your demand - evaluate availability of grid capacity and alternative sources, time to procure, cost and sustainability.



Evaluate connection timeline – consider innovative approval pathways, but build in realistic project timeline, with alternatives options, including different sites, power sources and use cases.



Assess if the operator can implement power sharing, hedging or other arrangements to manage demand, and assess regulatory impact.



THEME 2

Going ‘green’: APAC is on the move, and many investors demand it

All markets covered in this Guide have ratified the Paris Agreement and the Kyoto Protocols, making commitments to reduce carbon emissions.

However, these international commitments generally do not translate into regulatory requirements on data centre developers and operators to ‘go green’. This is despite the outsized consumption of energy and water by data centres.

Instead, there is a focus on power usage effectiveness (**PUE**) as a metric to gauge the sustainability of data centres, with several jurisdictions imposing targets or mandatory limits on PUE for new data centres:

- **Singapore** – the DC-CFA scheme requires a PUE of 1.3 or lower
- **Vietnam** – a target PUE of 1.4 or lower
- **Japan** – planning approvals require a PUE of 1.4 or lower by 2030
- **Malaysia** – a target PUE of 1.4 or lower for hyperscale data centres
- **China** - data centres for government require a PUE of 1.3 or lower.



ON THE GROUND

UNLOCKING GREEN POWER WITH CORPORATE PPAS

Vietnam

Recent reforms on direct PPAs represent a significant milestone, facilitating direct sales of renewable energy and demonstrating Vietnam's commitment to achieving net zero emissions by 2050.

Malaysia

The government's Corporate Renewable Energy Supply Scheme (**CRESS**) allows corporate customers to enter into corporate PPAs with utility scale renewable generators.

Japan

Corporate PPAs are gaining momentum with Google recently signing its first renewable energy purchase deals, including an agreement with Itochu Corporation for small-scale solar plants across multiple grid regions and a 20MW project with Shizen Energy.

These agreements help data centre operators (and their clients) meet sustainability goals while providing financial stability through fixed energy prices, addressing both environmental objectives and energy security concerns that impact business operations across developed and developing Asian markets.



Lean into the ‘green’ opportunities where local policy and capacity align (for example, renewable power sources, sustainable cooling, or innovative tech). Explore corporate PPAs to secure renewable energy sources.



Monitor PUE regulations and targets to maintain compliance and improve sustainability.



Consider investor pressures and global trends towards sustainability in decision-making processes.

THEME 3

Water: keeping our cool

Data centre IT equipment generates an incredible amount of heat and requires constant cooling to maintain an operating temperature, and to avoid outages.

While power has taken centre stage for regulatory intervention across the markets discussed in this Guide, water usage is emerging as a growing area of focus.

Water availability is a pressing concern, especially in Australia and parts of Indonesia and Malaysia. Innovative cooling systems, such as using recycled water or advanced air or liquid cooling technologies, are gaining traction. These measures not only address environmental concerns but also drive operational efficiency.

Improved **water efficiency** is a major focus of innovation efforts for data centre operators and the supply chain that supports them. For example, liquid cooling systems have emerged to cool high-performance chips such as GPUs. These are closed loop systems, which can reduce the amount of water that evaporates, increasing water efficiency.

In several markets, planning authorities consider how a data centre operator plans to incorporate water-efficient systems into its operations when assessing an application for planning approval.

Data centres are not alone in demands for water

For many jurisdictions in this Guide, particularly in Southeast Asia, agriculture remains an important economic sector that is also dependent on access to large amounts of water.

Governments in those jurisdictions have competing water policy demands as they seek to encourage data centre investment (often to support policies of digitisation and economic development) without undermining the agricultural sector that sustains their export economies. Addressing these policy tensions is important when seeking approvals to build data centres in the region.



ON THE GROUND

WORKING WATER INTO APPROVALS

Singapore

Water efficiency is considered as part of any DC-CFA process. Data centre operators have been awarded capacity in Singapore where they have deployed cutting edge cooling technologies.

Malaysia (Johor)

There have been shortages of potable water in recent years in the peninsula – which has coincided with the explosive growth of its data centre market. The National Water Services Commission (or **SPAN**) has recommended that local authorities assess the availability of water including alternative water resources when considering planning approval for a data centre.

Malaysia’s Guidelines for Sustainable Development of Data Centres also contains water usage effectiveness (**WUE**) targets (consumption of 2.2 m³ of water per MWh for hyperscale facilities) and encourage the use of reclaimed water.

Australia, Hong Kong, Thailand, India and the Philippines

Planning authorities also consider the availability and wastewater impact of a data centre as part of the approval process for the relevant site.



Check compliance with any water rights grants and licensing frameworks, and assess additional steps to be factored into project timetables. Engage with planning authorities early.



Consider implementing water-efficient cooling systems in data centre designs, and procuring water from alternative sources.



Assess local water scarcity issues and water policy trends and consider if they may impact data centre usage, or profitability.

1. Mytton, D. Data centre water consumption. npj Clean Water 4, 11 (2021), <https://www.nature.com/articles/s41545-021-00101-w>



THEME 4

Show me the (government) incentive, I'll show you the outcome

Incentives can make or break investment decisions. **Malaysia** offers tax holidays to attract data centre investments. Meanwhile, **Indonesia** facilitates faster permits and land acquisition processes. These incentives not only lure investors but also foster a competitive environment for data centre growth.

Developed economies like **Australia, Japan, South Korea and Singapore** are natural targets for data centre investment, with advanced economies, strong legal frameworks, high levels of international and domestic connectivity and talent density. Investors are extremely keen to allocate capital to those markets.

Other jurisdictions in the region therefore often work harder to attract capital. Governments in those jurisdictions are more likely to create investment incentives and regulatory settings designed to attract the capital, skills, technology and ecosystem needed to expand the domestic data centre market, including by offering:

- tax incentives such as reduced tax rates, tax exemptions, tax holidays or tax offsets for qualifying spending
- grants or subsidies for expenditure on data centre research, construction or operations
- discounts on rental and utility payments
- streamlined land access, zoning, permitting or utilities
- exemptions to foreign ownership controls for land or facilities, and
- relaxed immigration and visa requirements to attract a skilled workforce.

Incentive programs vary across the APAC region. However, there are a few common approaches: special economic zones and special status.

Building data centre ecosystems with SEZs

Across the region, industrial or high-tech parks are becoming enhanced into SEZs to encourage data centre investment. At their most basic, these SEZs provide access to the infrastructure and services needed for a data centre ecosystem including power, water, telecommunications and road infrastructure. However, government authorities may also offer incentives and benefits, such as those mentioned above.

Special status to attract targeted investments

Some incentives provide special status that is not linked to any specific zone or area.

Malaysia

Eligible data centre businesses in Malaysia can seek approval for ‘Malaysia Digital Status’. This provides access to a number of tax concessions, including income, investment and sales tax exemptions and allowances. Additionally, the Digital Ecosystem Acceleration Scheme (**DESAC**) provides other, separate capital allowances to apply against taxable income for data centre operators that meet certain criteria, such as local employment commitments and green technology deployments.

Singapore

‘Pioneer’ businesses that bring new technology can access income tax exemptions and reduced tax rates, and those who expand high-value infrastructure in Singapore can seek reduced corporate income tax rates as low as 5-10%.

Indonesia

Investments in the digital economy, including data processing and hosting activities, can qualify for a tax allowance under the *Minister of Finance Regulation* No. 130/PMK.010/2020. This incentive requires a minimum investment of IDR100 billion (~US\$6.1 million).

Japan

As part of the government’s decentralisation efforts, subsidies are available for projects on ≥10 hectares of land, covering up to ¥15.54 billion (~US\$108 million) to off-set infrastructure-related costs, and for up to ¥30 billion (~US\$208 million) for both infrastructure and facility construction-related costs.

Vietnam

The Investment Support Fund (**ISF**) is designed to provide financial incentives for high-tech enterprises, including high-tech data centre developments and operations. The ISF offers annual expense support and initial investment cost support.

- ✓ Consider (early) leveraging tax incentives, grants, subsidies and SEZ benefits.
- ✓ Assess whether structural needs to meet the requirements for an incentive (for example, a required site location) are practical and ultimately useful.
- ✓ Assess if there are any neutralising or negative factors of pursuing an incentive, including to compliance in other areas, other jurisdictions, or with other stakeholder expectations.

Examples of SEZs across the markets covered in this Guide

JURISDICTION	NAME/LOCATION	FINANCIAL INCENTIVES	NON-FINANCIAL INCENTIVES
CHINA	Shenzhen, Zhuhai, Shantou, Xiamen, Hainan, Khorgos	Reduced corporate income tax rates and tariff exemptions	Flexible land use policies and cross border capital facilitation
INDIA	Maharashtra, Karnataka, Tamil Nadu and Uttar Pradesh	Tax exemptions like duty free procurement of goods/ services	Infrastructural support
INDONESIA	~ 20 SEZs	Relaxed VAT, import tax, excises and regional tax	Streamlined import restrictions, relaxed building licenses
MALAYSIA	Johor-Singapore SEZ	Special corporate tax rate for AI supply chain businesses	-
PHILIPPINES	Clark SEZ	Tax holidays, tax exemptions on imported goods, tax credits	Simplification of customs procedures, employment of foreign nationals
VIETNAM	Saigon Hi-Tech Park	Tax breaks	Land leases and support services



THEME 5

Understanding foreign investment controls

International capital is a critical driver of data centre growth in the APAC region. In emerging economies, particularly where domestic capital and expertise are limited, foreign investment is pivotal for delivering the digital infrastructure required to meet rising demand for data services.

It also supports broader economic goals - stimulating growth, digitising the economy, creating jobs, fostering innovation and bringing in expertise and advanced technologies that can improve operational efficiencies and service quality.

GOVERNMENTS ACROSS APAC INCREASINGLY RECOGNISE THESE BENEFITS. COUNTRIES SUCH AS VIETNAM, INDIA AND THE PHILIPPINES ARE ACTIVELY REFORMING OR CLARIFYING THEIR REGULATORY FRAMEWORKS TO ATTRACT FOREIGN CAPITAL AND EXPERTISE.

Private capital, from global infrastructure funds to strategic investors, is also responding. With a strong appetite for risk-adjusted returns, these investors are targeting both mature markets with proven demand and emerging markets offering first-mover advantage.

In turn, this reinforces the pressure on governments to ensure their regulatory regimes support and enable foreign participation.

Diversity in regulation

Despite this trend toward liberalisation, foreign investment regulation across the APAC region remains highly diverse. Jurisdictions range from open and investor-friendly, to those with complex restrictions influenced by concerns around sectoral sensitivities, land ownership, national security and domestic industry protection.

The regulatory frameworks in place can either serve as a catalyst or barrier, influencing the scale and nature of investment in the region.

Approaches to foreign investment controls

JURISDICTION	KEY FEATURES
LIBERAL REGIMES	
SINGAPORE AND HONG KONG	Allow 100% foreign ownership of data centres.
SOUTH KOREA	Few restrictions on land acquisition or data centre ownership, aside from facility-based telecommunication services.
CONDITIONALLY OPEN REGIMES, WHERE CONTROLS LIKE APPROVALS, NOTIFICATION OR LOCAL PRESENCE REQUIREMENTS, APPLY	
JAPAN	No restriction on land ownership, but approval is required.
INDIA	Requires, amongst other things, government approval for investors from neighbouring countries; mandates a local presence for ownership of immovable property.
TAIWAN	Permitted with approval, but restrictions imposed on PRC investment.
STRINGENT REGIMES	
AUSTRALIA	Requires Foreign Investment Review Board (FIRB) approval for land and data centre investments, with national security scrutiny for investments in critical infrastructure.
CHINA	Caps foreign ownership in relation to data centres operations at 50%, excluding qualifying Hong Kong or Macau foreign investors; foreigners cannot own land but can obtain long-term land use rights.
THAILAND	Foreigners generally cannot own land and must secure Board of Investment approval to do so; Foreign Business Licence or Foreign Business Certificate also required to developer or operate data centres.

Finding the right pathway




The complexity of APAC’s regulatory landscape means foreign investment strategies must be carefully structured. Fragmented controls across land ownership, operating licences and critical infrastructure often require nuanced legal and commercial analysis and navigation. For example, in the **Philippines**, while 100% foreign ownership of data centres is allowed, foreign ownership of land is capped at 40% - though long-term leases are a permitted pathway.

This patchwork of regulation often leads foreign investors to pursue **local partnerships or joint ventures**, particularly in jurisdictions where:

- land ownership is restricted (for example, **China, Thailand** and **Vietnam**)
- operational licences are available to foreign investors, but land, infrastructure or telecommunications constraints apply (for example, **Malaysia**), or
- cultural sensitivities and business norms add complexity (for example, in **South Korea and Japan**, which remain quite local markets).

However, the benefits of local partnerships extend beyond compliance – they also include accelerated market entry, risk sharing and invaluable in-market insight.

SUCCESS FOR FOREIGN INVESTORS IN THESE MARKETS OFTEN HINGES ON ALIGNING WITH LOCAL PARTNERS, UNDERSTANDING LAYERED REGULATORY REGIMES, AND STRUCTURING INVESTMENTS THAT REFLECT BOTH LEGAL LIMITS AND MARKET REALITIES.

-  Consider (early) any relevant foreign ownership controls – these may apply to land, facilities, operations or even licences. Understand the triggers for approvals or notifications.
-  Identify if local partnerships are required to navigate ownership restrictions.
-  Align investment strategies with local norms and regulations to ensure compliance and optimise your market entry or expansion.

Foreign ownership of data centres and land

JURISDICTION	IS FOREIGN OWNERSHIP PERMITTED?	
	DATA CENTRES	LAND
AUSTRALIA	Yes, subject to approval by the FIRB and restrictions under the Hosting Certification Framework (HCF)	Yes, subject to FIRB approval and HCF restrictions
CHINA	Foreign ownership in data centre operations is capped at 50%, excluding qualifying Hong Kong and Macao investors	Possible for land use rights through long term leases
HONG KONG	Yes	Yes
INDIA	Approval is required for investments from neighbouring countries; otherwise yes	Restricted to investors with a local presence; and certain types of land cannot be acquired
INDONESIA	Yes	Yes for a right to build, similar to leasehold title
JAPAN	Yes, subject to government approval	Yes
MALAYSIA	Yes, but operational licences can only be held by a Malaysian entity with minority foreign ownership and minimum 30% Bumiputera equity	Yes with approval
PHILIPPINES	Yes	Yes via a local entity, and subject to a limit of 40% foreign ownership; long term leases otherwise permissible
SINGAPORE	Yes	Yes
SOUTH KOREA	Yes, but caps apply to ownership of facility based telecommunications providers	Generally yes, subject to some zoning restrictions
TAIWAN	Yes with prior approval, except for PRC investors, for whom ownership is prohibited	Yes only through a locally incorporated entity
THAILAND	Only with a Foreign Business Licence or Foreign Investment Certificate	Prohibited, subjected to limited exceptions, including where Board of Investment provides approval and land is used for specific Board of Investment promoted business
VIETNAM	Yes; some ownership caps for certain telecommunication service providers	Land cannot be privately owned, but no restrictions on land use rights



THEME 6

Local demand (not data localisation requirements) is driving investment onshore

Most jurisdictions have requirements to keep certain data onshore, or impose restrictions on data exports. This is common, for example, in relation to sensitive government data, financial information or health information. Some jurisdictions go further.

There is ample media and social commentary suggesting that data localisation measures are having the effect of driving data centre investment onshore in the jurisdictions where they are made.

The thesis behind this commentary is that cloud service providers and global technology companies cannot sustain a regional gateway model (servicing the APAC region from one jurisdiction or a small number of jurisdictions) if they must retain large amounts of data onshore, and therefore must construct data centres in-country to respond to capacity demands and other local requirements.

The survey of markets in this Guide revealed more nuance to this story, with impacted markets such as Vietnam and Indonesia having some of the world’s largest and fastest growing populations, it is more likely that market forces, in the form of increasing consumer demand for digital products and cloud services, are predominantly doing that work - with the help of government policies and regulations supporting foreign investment, digital transformation and infrastructure development.

However, this may change if AI sovereignty initiatives take hold (see Theme 8 below).

- ✓ Monitor data localisation laws that could impact data centre operations.
- ✓ Focus on market-driven growth opportunities fuelled by increasing digital demand, rather than viewing data localisation as a business opportunity in itself. Map realistic local need.
- ✓ Assess if the policy and regulatory pipeline indicates an expansion, or contraction, of localisation rules to address sovereignty, capital attraction or other policy objectives.

THEME 7

Data centre growth is intertwined with export controls

Export controls are a reality for data centre investors. These regulations affect the availability of cutting-edge technologies, and they can delay projects. Investors must navigate these controls to ensure smooth operations and compliance.

The global expansion of data centres is being reshaped by AI export controls, given that most advanced AI chips and technologies are of US origin. Data centres also often use highly regulated commodities and/or 'dual use goods' which adds complexity.

Over time, but with a significant escalation in the past few years, the US has introduced sweeping restrictions on the export, re-export and transfer of advanced AI technologies aimed at safeguarding national security and preserving its technological lead in AI. These include:

- hardware controls on high-performance chips, and
- measures like the AI diffusion rule ([though now rescinded](#)), which sought to restrict access to powerful AI models trained on US technology.

These export controls have significant implications for data centre operators and investors in the APAC region, where access to cutting-edge AI hardware and infrastructure is critical to growth and competitiveness.

FOR NOW, MANY ADVANCED AI TECHNOLOGIES REMAIN OF US-ORIGIN, AND EXPORT CONTROLS WILL CONTINUE TO SHAPE WHERE AND HOW DATA CENTRES ARE BUILT AND OPERATED ACROSS THE APAC REGION.

Operators and investors must closely track regulatory developments and account for potential restrictions on chip access when planning infrastructure, particularly for AI-optimised or GPU-intensive facilities.

Navigating this shifting landscape underscores the need to stay agile - balancing geopolitical risks with the potential upside of rising local innovation and diversification.



ON THE GROUND
KEEPING DATA CLOSE

Vietnam has national and cyber security motives

There is a move towards requiring data localisation for a wide range of consumer-related data. Domestic providers of telecommunications, internet, cloud computing or data storage services (including data centre operators) must store copies of certain personal data, user-generated data (like account names, service usage time, credit card details, email and IP addresses, and registered phone numbers) and other information within Vietnam.

In 2024, this localisation requirement was extended to apply to foreign providers of cloud computing and data centre services when operating in Vietnam. The Law on Data will expand this localisation requirement further still by restricting the offshore transfer of certain important data. A significant purpose stated for this localisation is to assist in cyber security investigations and national security matters.

Indonesia tightens net on sensitive data

Recent reforms have distinguished electronic system operators (being cloud service providers and data processors) that service the government from those that service the private sector only, with the former being required to carry out all data processing onshore.

Private-sector only electronic system operators are generally permitted to host data offshore, provided they give government authorities access to it. This is excepting industries - financial services and health - where data is considered especially sensitive.

Financial service providers such as banks, insurers and non-bank lenders are subject to additional industry-specific onshoring requirements, unless they obtain an exemption from the Financial Services Authority. Healthcare facilities are required to store data in Indonesia without exception.



ON THE GROUND
HEAT STILL ON FOR CHINA AND HONG KONG

China and Hong Kong continue to face the most stringent limitations. In response, Chinese AI companies have adopted alternative solutions - such as moving training data offshore to markets like Malaysia, where they lease servers equipped with US-made chips to train models. At the same time, China is doubling down on self-reliance, intensifying investment in domestic AI capabilities.

Huawei has made notable progress in developing AI chips that could eventually reduce reliance on US technology. This push for self-reliance presents both a challenge and an opportunity for other players in the region, as new ecosystems and supply chains begin to emerge.

Further afield in Asia, countries will likely see their access to US-originating AI technology bundled into negotiations with the US in relation to tariffs and trade. Access will require political alignment with the US and may lead to making some difficult decisions given the need in the APAC region to balance relationships with both the US and China.

- ✓ Track ongoing developments in US export controls, especially concerning access to US-originating AI technology and controls on GPU-as-a-service models. This is a moving feast.
- ✓ Implement a strong trade compliance framework covering export controls, sanctions and dual-use goods, with alternative sourcing strategies to mitigate technology access restrictions.
- ✓ Craft tailored contractual protections that go beyond a duty to ‘comply with applicable law’ and address specific regulatory risks.

THEME 8

The data centre opportunity for national security and AI sovereignty

Data centres are strategic assets. They support national security and data sovereignty.

In Indonesia, the government is investing in data centres to ensure data sovereignty and boost its digital economy. Australia is focusing on securing its data centre infrastructure as part of its national security strategy. These moves underscore the critical role of data centres in safeguarding national interests.

Industry leaders and governments around the world are increasingly convinced that AI technology will be a lynchpin of economic success in the future, but there’s a lot of upfront investment required to reap the benefits.

Concerns are shaping government strategies

Given the competitive advantages that are expected from AI technology and the uncertainty in the global political and economic landscape, many governments are nervous about becoming reliant on AI infrastructure, large language models (LLMs) and products based overseas. This is due to:

- the potential limited access to the resources, and
- the risks associated with transferring to an overseas operator the necessary amount of sensitive domestic data to reap the benefits of the technology.

TAIWAN AND THE SINGAPORE-JOHOR SEZ IN MALAYSIA HAVE TAX CONCESSIONS SPECIFICALLY INTRODUCED TO BRING IN AI-RELATED BUSINESSES. OTHER JURISDICTIONS LIKE AUSTRALIA ARE IN THE PROCESS OF DEBATING AND IMPLEMENTING AI GOVERNANCE FRAMEWORKS.

Data centre capacity is a key resource to achieve AI sovereignty goals. However, our anecdotal experience is that this focus on AI sovereignty seems to be manifesting at the level of policy rather than direct investments at this stage. Jurisdictions in the APAC region are at different levels of progression in their AI sovereignty strategies.

The inevitable rise of AI

McKinsey forecasts that demand for data centre capacity generally is likely to increase by around 22% year on year to 2030, putting total global demand in 2030 at roughly 3 times current demand. To meet that demand will require a significant increase in the rate at which new capacity is brought online.

AI-specific data centre capacity is expected to rise even faster - 33% year on year. Yet much of the existing data centre capacity is not capable of supporting the density of computing power demanded by AI without significant retrofitting and re-engineering of existing sites to meet the power and cooling demands that come with that intense computing.

Accordingly, AI-ready data centre capacity is an enticing investment opportunity in the region. Early movers may reap significant benefits if they can bring capacity to market to then fund further expansion throughout the region.

A key question for any AI sovereignty initiative is how it will be implemented. Currently, all of the top LLMs are either developed in the US or China. If sovereign AI capability is deployed using one of those LLMs – which may be a commercial and technical reality – that decision may come with geopolitical consequences, in much the same way as acquiring military hardware. Will AI sovereignty really be about political alignment to the US or China?

- ✓ Consider impact of national security policies and regulations when planning data centre locations and operations.
- ✓ Stay informed with evolving government AI strategies and potential impacts on data centre needs, including new opportunities for investment in AI-ready infrastructure.
- ✓ Explore local opportunities or partnerships where foreign investment faces regulatory hurdles.

TO ADDRESS THESE RISKS, MANY GOVERNMENTS ARE TURNING THEIR FOCUS TO AI SOVEREIGNTY – THE IDEA OF INVESTING IN LARGE-SCALE DOMESTIC AI DEPLOYMENTS TO ENSURE SECURE SUPPLY IN THE FUTURE AND GREATER CONTROL OVER HOW THE AI TECHNOLOGY MIGHT BE USED.

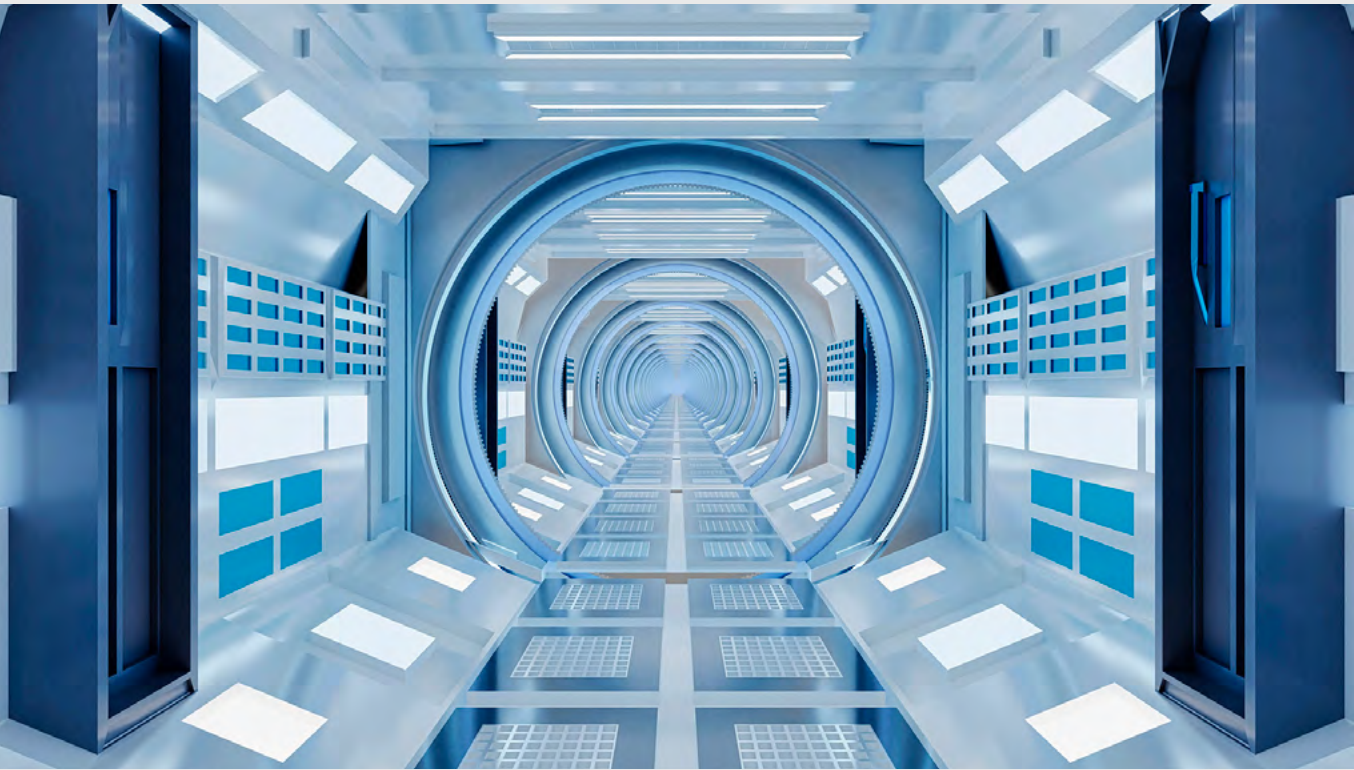
DATA CENTRE CAPACITY
PROJECTED GROWTH TO 2030

22%

year on year
at least 3x current demand

AI-SPECIFIC
33%

year on year growth



A REGIONAL SNAPSHOT

What does the regulatory landscape look like - in one heatmap? We've collated the settings captured throughout this Guide to give you a high-level view of how investor-friendly jurisdictions are across key issues - from very (little to no regulation), to not at all (significant regulatory restrictions).

Status / Regulation

- Little to no regulation, or investment-friendly
- Standard regulation across markets
- Some hurdles, but manageable with compliance
- Significant restrictions or hurdles

ISSUE	AUSTRALIA	CHINA	HONG KONG SAR	INDIA	INDONESIA
POWER ACCESS	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>
WATER ACCESS	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>
LAND: EASE OF ACQUIRING	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>
TELECOMMUNICATIONS REGULATIONS	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>
FDI: ACCESSIBILITY FOR FOREIGNERS	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>
INCENTIVES	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>
DATA PROTECTION & CYBER SECURITY	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>
CRITICAL INFRASTRUCTURE REGULATIONS	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>
DATA LOCALISATION	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>
ESG REPORTING & COMPLIANCE	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>

What did we find?

Malaysia, India, Vietnam, and Indonesia present both opportunities and challenges. Thailand is emerging as an attractive location. Singapore and South Korea offer appealing incentives, tax benefits and supportive digital economy policies, offering more reliable investment decisions.

Conversely, regulatory nuances in areas like energy procurement, land acquisition and data localisation, especially in markets like China, can pose significant hurdles.

BY NAVIGATING THESE COMPLEXITIES WITH FORESIGHT, YOU CAN CAPITALISE ON THE BENEFITS THAT THESE VIBRANT MARKETS OFFER, ENSURING DATA CENTRE OPERATIONS ARE COMPETITIVE, COMPLIANT AND COMMERCIALY SUCCESSFUL.

JAPAN	MALAYSIA	PHILIPPINES	SINGAPORE	SOUTH KOREA	TAIWAN	THAILAND	VIETNAM
<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>
<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>
<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>
<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>
<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>
<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>
<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>
<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>
<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>
<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>



AUSTRALIA

CHAPTER 1

SNAPSHOT



Australia's data centre market is anticipated to double in size in the next 5 years. With its stable economy, transparent regulatory framework and high quality 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 (particularly from government and financial services tenants, and increasingly hyperscalers) as a mature developed economy.

However, the allure of the Australian market is marked by insufficient carrots and burdensome sticks. Australia's strict foreign investment regulations can significantly extend the timeline for site acquisition for foreign investors and developers, as well as the timelines for foreign hyperscale tenants to commence a tenancy in the site. Power supply continues to be a concern. Critical infrastructure regulations and government security requirements increase the regulatory burden.

There are also limited incentives offered by government to encourage investment. Despite these impeding factors, a remarkable data centre growth story is emerging.

OPPORTUNITIES

- ✓ Stable economy
- ✓ Clear regulatory landscape
- ✓ Relatively unrestricted access to advanced AI chips and model weights

CHALLENGES

- ✗ Power supply constraints
- ✗ Foreign investment controls
- ✗ No incentives

SPOTLIGHT ON KEY DRIVERS

STABLE ECONOMY WITH A CLEAR REGULATORY LANDSCAPE

Australia boasts a stable economy with a transparent regulatory framework, providing clarity and certainty for data centre development.

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.

POWER SUPPLY CONSTRAINTS

Australia's data centre development faces the spectre of power supply constraints hindering growth.

The impending shutdown of major coal power stations, combined with network areas already at capacity and the skyrocketing energy demands of new data centres, threaten to create a shortfall in supply. This also presents challenges for connecting large new electricity loads.

Addressing these constraints, especially when transitioning to renewable energy, will be crucial for supporting the growth of data centres in Australia.

LIMITED INCENTIVES AND SIGNIFICANT FOREIGN INVESTMENT RESTRICTIONS

In comparison to other countries, the Australian Government offers significantly fewer incentives and benefits to data centre developers.

Foreign investors must navigate complex regulations which can complicate and delay projects. Chief among these is the requirement for approval from FIRB for land acquisitions and data centre operations and the significant operational constraints imposed by the *Security of Critical Infrastructure Act 2018 (SOCI Act)* and the Federal Government's Hosting Certification Framework (**HCF**).

It is crucial for developers to carefully assess the FIRB, SOCI Act and HCF implications before committing to data centre projects in Australia.

'In the past 5 years Australia has dramatically evolved into a top destination for digital infrastructure and now ranks among the top five globally for data centre built-out capacity. We've seen investments surge, driven by major players.'

Cheng Lim
Partner
King & Wood Mallesons



OPERATIONAL

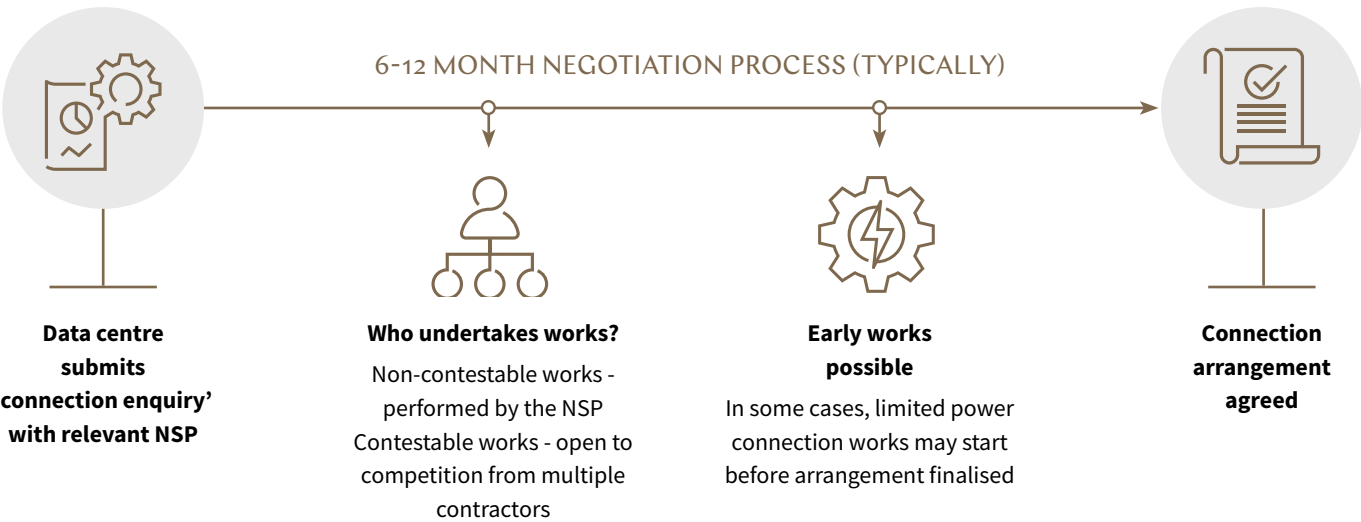
01. POWER

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 impending shutdown of large coal power stations and the forecasted massive energy consumption requirements of new data centres, and
- some parts of the NSPs' networks are **at capacity**, creating constraints on where large new electricity loads can be connected.



Power purchase agreements

In Australia, most corporate PPAs are structured as corporate virtual PPAs rather than corporate physical PPAs. 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 possible for a consumer to acquire electricity directly from a generator if the electricity needs to be wheeled through the grid. In these scenarios, all electricity must be bought and sold through the central market, operated by the Australian Energy Market Operator. In some circumstances, a corporate virtual PPA can be considered as 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 System (**NABERS**) energy rating, an Australian Government initiative. The NABERS rating 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. This aims to reduce greenhouse gas 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 Retailer Reliability Obligation may also require those 'liable entities' to procure **firmed electricity contracts** to cover a data centre's load in the event of forecasted supply shortfalls.

Technical access standards in the National Energy Market (**NEM**) National Electricity Rules will apply consistently across data centres (regardless of ownership structure) under revisions that take effect from 21 August 2025. 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 applicants **based on type** rather than owner or operator registration.

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 across the nation 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 or water entitlement** may be required in some situations, depending on the local jurisdiction.

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

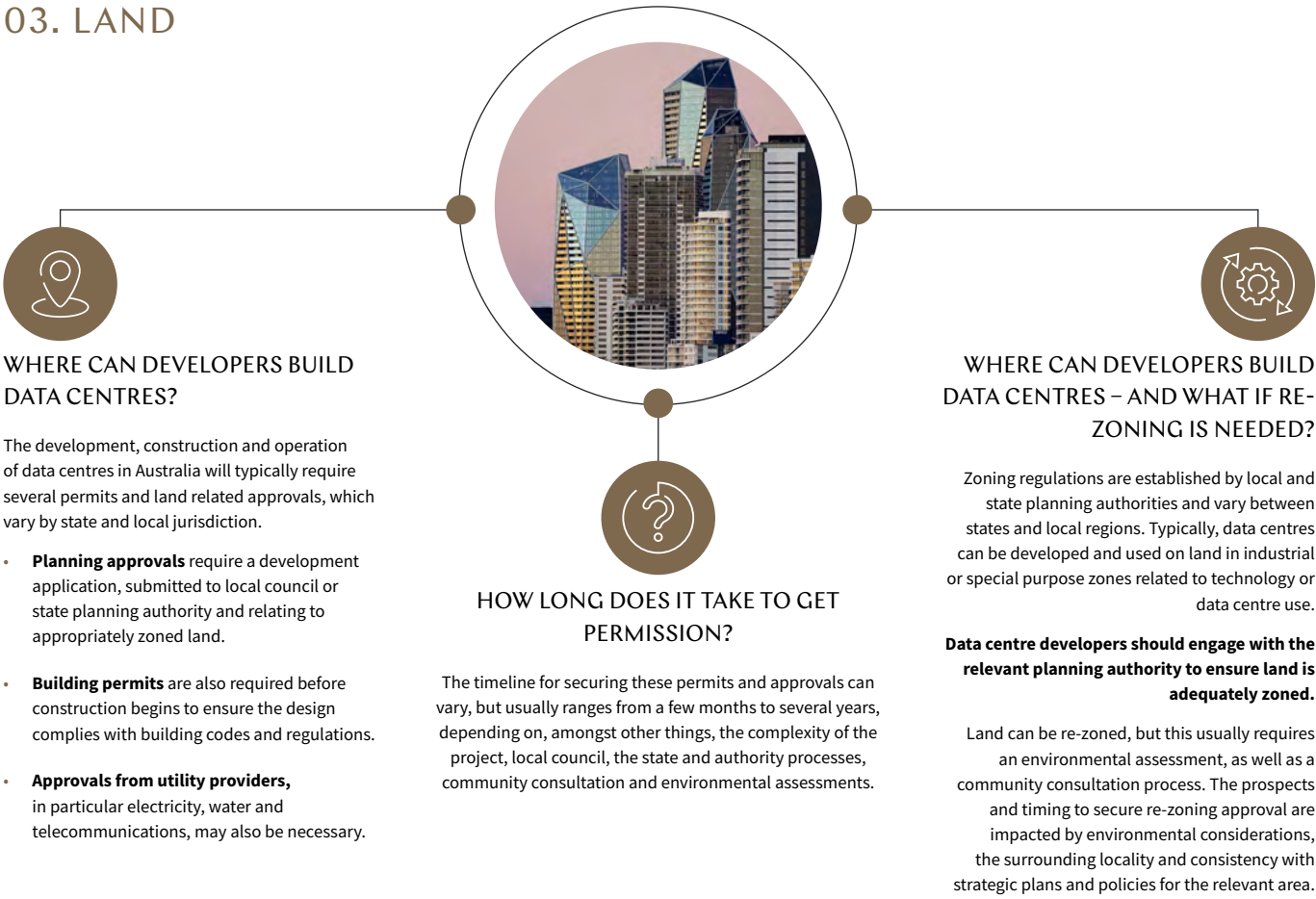
All developments, including data centres, must comply with general legal obligations relating to water, waste management and environmental and planning approvals. These obligations vary between each state, territory and local government.

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

For example, in New South Wales, 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, there are no efficiency, sustainability or social impact laws or regulations for the procurement or use of water specifically relating to data centres.

03. LAND



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’ (**DSPs**) in relation to national security or law enforcement matters.

Data centre operators may be considered DSPs, 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 DSPs requesting that they perform certain activities or to develop new capabilities to assist with investigations. Some notices (technical assistance notices and technical capabilities notices) are mandatory, while others (technical assistance requests) are voluntary.

The activities that can be requested of DSPs who are data centres include (relevantly):

- providing technical information relating to the data centre facilities such as design, manufacture information
- install, maintain or test software at the data centre
- give information to or assist law enforcement under a warrant or authorisation or in carrying out a warrant or authorisation
- provide access to software used in connection with electronic services, or facilities at its data centres, or
- conceal covert actions by law enforcement at its data centre.

Technical assistance cannot be requested by agencies to introduce a systematic weakness or vulnerability, 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 value-add services (VAS) supplied with a data centre service may also bring an operator in scope as a carriage service provider, such as an internet connectivity service.

STRATEGIC OPPORTUNITIES

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 a 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.

WANT A ‘PLAYBOOK’ TO WORK OUT – AND IMPROVE - THE PROSPECTS FOR A FOREIGN BID? CHECK OUT KWM’S 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. Businesses that are a responsible entity or direct interest holder in respect of critical infrastructure assets are ‘national security businesses’ (**NSB**).

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 by a foreign person in a data centre business that is a NSB, regardless of business value, and
- the starting of a new data centre business, that is a NSB, 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.





06. TAX AND OTHER INCENTIVES

Special economic zones

None.

Tax incentives

If a managed investment trust (**MIT**) invests in a data centre that obtains either a 6-star rating from the 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 7:30 pm AEST on 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 many have been owner/builders) to secure competitive space for data centres in the Australian market.'

COMPLIANCE AND RISK MANAGEMENT

07. DATA PROTECTION AND CYBER SECURITY

Data protection or privacy laws

The Australian Privacy Principles (**APP**) are the cornerstone of data protection and privacy, contained in 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). It would only apply, in that scenario, only in relation to personal information that the data centre itself holds (for example, about customer personnel). However, a hosting service provider may have obligations 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.

Cyber security laws

Responsible entities of data centres that are classified as critical infrastructure (see section 8 Critical infrastructure and security) **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 [Section 8](#) Critical Infrastructure and security below). 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,' which are then subject to enhanced cyber security obligations, including developing cyber security incident response plans, undertaking cyber security exercises, undertaking vulnerability assessments and providing 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 Australian national interest (including the economy, the functioning of government and public wellbeing), and in many cases, data centres may be considered such critical infrastructure.

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

- registering the data centre with the regulator (the Cyber and Infrastructure Security Centre)
- 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
- reporting cyber security incidents to the regulator (within very short timeframes) (see [Section 7](#) Data Protection and Cyber security above), 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** (see definition over the page) 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.



National security issues

- There are various national security considerations for data centres in Australia. Notably:
- under the Commonwealth **Government’s Protective Security Policy Framework (PSPF)**, Commonwealth government entities can only procure hosting services from providers that have obtained **HCF certification**, which extends to cloud services and the infrastructure underpinning those cloud services,
 - responsible entities, or direct interest holders, of data centres that meet the threshold of a ‘critical data storage or processing asset’ (see above) are considered ‘national security businesses’ under the FATA, and 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 [Section 5](#) Foreign Investment Restrictions above), and
 - 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).

Physical security issues

To obtain HCF certification - generally, a prerequisite for providing services to Australian government customers or supporting those who do - 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.

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.

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

Data centre operators and customers who are subject to the APPs (see [Section 7](#) Data protection and cyber security) 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 individuals consent, where expressly informed the APPs will not apply to overseas disclosure.

Commonwealth, state and territory government data

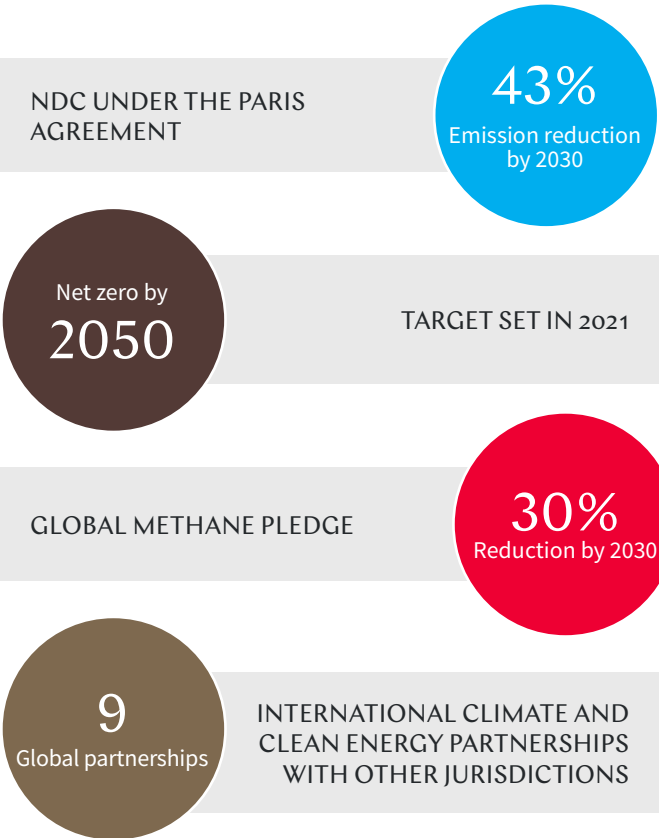
There are no explicit data offshoring restrictions on government data in legislation. However, Commonwealth and state governments will often have policies restricting data offshoring, or at least an implicit preference for their data to be stored in Australia.

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. 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 is due to submit a new NDC later in 2025 detailing 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 in data centres in Australia. However, as mentioned above, from 1 July 2025, 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)

Already required to comply (since 1 January 2025).

Entities must report if they meet at least two of the following:

- consolidated revenue of AU\$500 million or more
- consolidated gross assets of AU\$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, entities that are National Greenhouse Energy Reporting Scheme reporters 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 AU\$200 million or more
- EOFY consolidated gross assets of AU\$500 million or more, or
- EOFY FTE employees of 250 or more.

Alternatively, 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 AU\$50 million or more
- EOFY consolidated gross assets of AU\$25 million or more, or
- EOFY FTE employees of 100 or more.



11. SECTOR-SPECIFIC REGULATIONS APPLICABLE TO DATA CENTRES

Government bodies

Commonwealth entities must comply with the Protective Security Policy Framework, which requires any entities hosting official, sensitive and protected government information and data, and non-corporate Commonwealth entities when buying data centre space and services, to procure data centre and or cloud services from a HCF certified provider.

Obtaining such certification is a voluntary process and the [Australian Government provides guidelines](#) for how to assess readiness for certification.

Financial services providers or financial institutions

In Australia, financial services providers and financial institutions must comply with requirements relating to 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.

Digital asset service providers and digital certification bodies

Accredited service providers to the 'Gatekeeper Public Key Infrastructure Network' are required to be physically located within Australia and provide services from within Australia.



CHINA

CHAPTER 2

SNAPSHOT



China remains one of the most strategically important and tightly regulated data centre markets in Asia. Strong domestic demand - driven by AI adoption, cloud growth and digital transformation - continues to support large-scale infrastructure investment.

At the same time, operators must navigate complex challenges, including strict data localisation rules, cyber security obligations and foreign investment restrictions.

Government policy is a double-edged sword: while regulatory hurdles are high, supportive initiatives like 'East Data, West Computing' and green infrastructure mandates offer clear incentives for aligned operators.

However, escalating US export controls on advanced chips and technologies are adding pressure to high-performance data centre buildouts, particularly for AI and hyperscale workloads.

OPPORTUNITIES

- ✓ Supportive government policy
- ✓ Strong domestic demand

CHALLENGES

- ✗ Restrictive foreign investment framework
- ✗ Comprehensive data localisation rules
- ✗ US export controls

SPOTLIGHT ON KEY DRIVERS

NAVIGATING DATA LOCALISATION REQUIREMENTS

China enforces some of the world's most rigorous data localisation and cross-border transfer controls.

This is through the Personal Information Protection Law (PIPL), Cyber security Law (CSL) and Data Security Law (DSL). This is especially the case for operators of 'critical information infrastructure' (CII) and entities handling 'important data'.

These rules have compelled many multinational companies, such as Apple, to localise infrastructure, driving demand for compliant, onshore data centres.

FOREIGN INVESTMENT RESTRICTIONS

China maintains strict foreign ownership limits on data centre operations, particularly in relation to value-added telecommunications services (VAS).

This includes internet data centres (IDC) which is broadly defined to capture services including:

- hosting
- proxy maintenance
- system configuration
- server management and network-related services via outsourcing or leased data centre facilities, and
- cloud services.

Foreign investors (excluding qualified Hong Kong and Macao entities under the Closer Economic Partnership Arrangement (CEPA)) are generally capped at 50% ownership and face licensing barriers, such as ineligibility for the B11 VAS licence.

These restrictions limit direct market access for international operators, often necessitating joint ventures or partnerships to enter the Chinese market.

US EXPORT CONTROLS

US export restrictions on advanced semiconductors and AI-related technologies have directly impacted the availability of high-performance chips and servers for use in Chinese data centres.

These controls limit China's access to critical components from leading US and allied suppliers, affecting build-out timelines for AI and hyperscale infrastructure.

As a result, data centre investors in China must navigate increasing technology sourcing risks and compliance uncertainty, particularly for GPU-intensive applications.

'China's initiative to rapidly expand its data centre infrastructure driven by digitalisation and AI demand, with a strong focus on green energy integration, presents companies with substantial opportunities in energy-efficient solutions.'

Susan Ning
Partner
King & Wood Mallesons



OPERATIONAL

01. POWER

Getting power to a site

China’s electricity transmission and distribution are dominated by two state-owned utilities - the State Grid Corporation of China and China Southern Power Grid. Securing power for a data centre typically involves four key stages:

01

FEASIBILITY STUDY

02

PROJECT APPROVAL AND FILING

03

ENGINEERING AND CONSTRUCTION

04

GRID CONNECTION ACCEPTANCE

Requirements vary based on project size, location and entity type. Whether data centres are classified as commercial or industrial users, or large-scale energy-intensive projects, is determined on a case-by-case basis.

- **Residential users** have simplified processes (approximately 1-2 months), mainly involving review by the power company.
- For **commercial and industrial users**, supporting documents such as land use rights and environmental assessments must be submitted, with timelines ranging from 3–6 months.
- **Large-scale energy-intensive** projects may require multi-level approvals, which can take over a year.
- Projects in **remote areas** may face longer delays due to weaker grid infrastructure or local policy constraints.
- In designated **green pilot zones** (areas which comply with national or local renewable energy consumption policies, such as Inner Mongolia and Qinghai), renewable energy projects benefit from streamlined processes.

Power purchase agreements

Large electricity users, including data centres, are permitted to enter into, and are increasingly adopting, direct PPAs with power generation companies. These agreements offer long-term pricing certainty and access to renewable energy.

In 2024, the National Development and Reform Commission and the National Energy Administration issued the Basic Rules for Medium and Long-term Electricity Trading – Special Chapter on Green Electricity Trading.

These rules explicitly encourage large electricity users and electricity sales companies to purchase green electricity directly from power generators, further supporting the development of market-based renewable energy procurement.

In addition, a recent notice from the National Development and Reform Commission and the National Energy Administration issued in May 2025 authorises 'direct connection projects'. This means renewable energy generators can connect directly to certain large-scale consumers.

These combined changes may lead to significant shifts in the electricity procured by large electricity users in China and their practical implementation at different levels (national, local and provincial) will be watched closely.

Going ‘green’

China’s national and local governments strictly regulate data centre energy procurement and usage, emphasising green and low-carbon development.

The Special Action Plan for the Green and Low-Carbon Development of Data Centres (**Action Plan**) (July 2024) sets ambitious goals for energy performance.

By the end of 2025 new data centres in national hub nodes must use over 80% green electricity, and the PUE of new, renovated, or expanded large and hyperscale data centres must fall below 1.25.

The Action Plan promotes the following factors for low carbon development of data centres:

- optimised data centre layouts
- strict energy and water efficiency for new projects
- retrofit programmes for older facilities
- increased use of renewable energy
- efficient use of land and resources, and
- adoption of energy-saving technology and equipment.

The Action Plan also encourages the participation of data centres in **green electricity trading platforms** and **green certificate markets** to increase the share of clean energy in their supply mix. Relevant regions are encouraged to actively explore the development of direct supply of green electricity power supply arrangements, including:

- Inner Mongolia
- Qinghai
- Jiangsu
- Beijing-Tianjin-Hebei
- Yangtze River Delta
- Xinjiang, and
- Jilin

All government-procured data centres must comply with the Green Data Centre Government Procurement Demand Standards trial (**Green Data Centre Standards**). Key requirements include:

- **PUE thresholds:** Not exceeding 1.4 from 2023, and 1.3 from 2025 onward.
- **Renewable energy usage:** Minimum of 5% in 2023, 30% by 2025, and 100% by 2032.
- **Water efficiency:** Annual water consumption must not exceed 2.5L per kWh of electricity used by IT equipment.

02. WATER

Water supply

Water usage by data centres is regulated under the Green Data Centre Standards. The standard caps the water-to-energy ratio at 2.5 litres per kWh of electricity consumed by IT equipment, aiming to improve overall water efficiency in cooling and facility operations.

Water conservation policies

In addition to the Green Data Centre Standards, national and local policies, including the Action Plan for Green and Low Carbon Data Centres, encourage (but do not mandate) data centres to adopt water-saving technologies and optimise water use. This includes retrofitting for water efficiency and increasing the use of recycled or reclaimed water for cooling and other non-potable applications, particularly in regions facing water stress.



03. LAND

Permits and approvals

The development of data centres broadly follows general real estate project procedures. Key requirements include obtaining land use rights, project approval and filing, environmental impact assessments, land and engineering planning approvals, construction permits and completion acceptance.

The approval process generally involves two main stages: **pre-construction and project acceptance**.

- During **pre-construction**, the key milestone is obtaining the Construction Project Planning Permit, which requires submission of land ownership documents, design proposals and other supporting materials.
- In the **construction phase**, developers must ensure ongoing compliance with noise pollution laws (including the *Noise Pollution Prevention and Control Law* and local emission standards) and maintain safe and orderly construction practices to avoid suspensions, rectification orders or delivery delays.
- The **acceptance stage** begins with planning compliance verification (as required under Article 45 of the *Urban and Rural Planning Law*) to confirm adherence to approved plans, which is followed by:
 - Fire Safety Acceptance/Record-filing:** Either mandatory inspection, or record-filing with random checks, overseen by housing and urban-rural development authorities
 - Environmental Acceptance:** Self-conducted, with public disclosure of monitoring reports and regulatory oversight
 - Completion Acceptance and Record-filing:** Submission of completion reports, quality warranties, and relevant certificates to the competent authority, and
 - Land-use Compliance Verification:** Audit of land boundaries and fulfilment of land use contract obligations.

Zoning requirements

Data centre zoning is influenced by factors such as energy availability, climate, infrastructure, environmental risk and national or regional policy. Under the '*East Data, West Computing*' initiative, priority is given to building data centres in national hub nodes of the integrated computing network (for example, in Guizhou, or Inner Mongolia).

Several major cities have issued policies prohibiting new data centre projects in designated zones, such as the central urban areas of Beijing and Shanghai.

New developments in these restricted areas cannot be filed with the local Development and Reform Commission, effectively blocking project approval. Exceptions exist, primarily for government data centres, which may operate in restricted zones (for example, in central Beijing).

Expansion limitations

Expansions, reconstructions or increases in cabinet capacity in existing facilities within restricted zones may still trigger filing requirements. Where a project is located in a prohibited area, the likelihood of obtaining approval for such changes is low. Early and proactive engagement with the local Economic and Information Bureau and the Development and Reform Commission is essential, though there is currently no pathway for re-zoning.

04. TELECOMMUNICATIONS

Applicability of telecommunications laws to data centres

Data centres are regulated under national telecommunications laws and classified as providers of VAS. Two key instruments apply:

- the *Administrative Measures for Telecommunications Business Operation Licenses* set out the conditions, documentation and procedures required to obtain a VAS licence, and
- the *Telecommunications Business Classification Catalogue (2019 Edition)* classifies IDC services as a Class I VAS business (**B11**).

Is a telecommunications licence required?

Entities operating IDC services must obtain a Value-Added Telecommunications Business License (**B11 licence**). Core application requirements include:

- adequate funding, qualified personnel and registered premises
- availability of appropriate facilities and technical infrastructure, and
- a comprehensive information security management plan.

If a data centre operator outsources network equipment maintenance or management to a third party, that party must also hold a valid VAS license for the relevant activities.

A data centre which is self-built and self-operated, and does not provide services to third parties, does not require a B11 licence.



STRATEGIC OPPORTUNITIES

05. FOREIGN INVESTMENT RESTRICTIONS

Land

Foreign investors cannot own land in China, except for 'self-use' or 'self-residence' purposes in certain limited circumstances. They may otherwise only obtain land use rights through long-term leases.

Data centres

Under the CEPA signed in 2003, IDC and cloud computing services in Mainland China are open to qualified Hong Kong and Macao investors, who may hold a higher equity stake than the 50% cap that generally applies to other foreign investors. To qualify, such Hong Kong and Macao investors must:

- be registered or established in Hong Kong or Macao,
- have conducted substantive business operations for at least 3 years, and
- provide a verification certificate from the relevant telecommunications authority confirming the nature and scope of their services.

These investors may apply for the B11 value-added telecommunications licence (covering IDC and cloud services) under the *Telecommunication Services Classification Catalog*. The B11 licence remains unavailable to investors from other countries or regions.

Telecom sector access

Foreign ownership in VAS, including IDCs and cloud computing, is generally limited to 50%, and basic telecommunications services must remain Chinese-controlled.

These restrictions are set out in two core legal instruments:

- the *Special Administrative Measures for Foreign Investment Access (Negative List) (2024 Edition)*, applicable nationwide, and
- the *Negative List for Pilot Free Trade Zones (2021 Edition)*, applicable in designated free trade zones.

Certain services, such as e-commerce, call centres, domestic multi-party communications and store-and-forward services, are exempt from the 50% cap.

06. TAX AND OTHER INCENTIVES

Special economic zones

China has established several SEZs, including Shenzhen, Zhuhai, Shantou, Xiamen, Hainan, Kashgar and Khorgos, to attract foreign investment and support regional development. These SEZs offer preferential policies, such as:

- reduced corporate income tax rates
- tariff exemptions
- flexible land use policies, and
- cross-border capital facilitation.

The Hainan Free Trade Port, for example, applies a zero-tariff policy for certain imported goods and offers a reduced corporate tax rate of 15% for qualified enterprises.

Data centre incentives

Various local and provincial governments in China offer tax incentives, subsidies and grants to data centre operators and developers. These include VAT refunds or exemptions for enterprises engaged in data processing, storage and other eligible IT services.

Additional incentives are available for green and low-carbon initiatives. For example, Heilongjiang province and districts in Shanghai and Guangzhou offer one-off rewards of RMB1 million (approximately US\$140,000) to businesses recognised as national green factories or green supply chain enterprises.

US export controls continue to restrict China's access to advanced AI chips and technologies, with rules evolving rapidly. Despite the US government's decision to rescind the AI diffusion rule, it remains clear that China is the primary target of ongoing restrictions.

In response, China is intensifying investment in domestic AI capabilities, with companies like Huawei making notable progress in AI chip development. This push for technological self-reliance presents both a challenge and an opportunity for other players in the region, as China seeks to close the gap left by restricted foreign access.



COMPLIANCE AND RISK MANAGEMENT

07. DATA PROTECTION AND CYBER SECURITY

Data protection or privacy laws

Under the PIPL, data centre service providers typically act as entrusted personal information processors, assisting clients (referred to as ‘personal information handlers’) in meeting their data protection obligations.

A data processing agreement is required between the parties, outlining respective roles, responsibilities and liabilities.

Where the personal information handler does not directly control security measures, the data centre operator assumes primary responsibility for implementing technical and organisational safeguards.

Obligations include:

- appointing a data security officer and team, implementing data security policies
- regularly conducting risk assessments, monitoring, emergency drills and training
- vetting key personnel
- managing complaints, and
- reporting data disposal plans in scenarios such as dissolution or bankruptcy.

Cyber security laws

All data centres must comply with China’s Multi-Level Protection Scheme (**MLPS**), which classifies IT systems based on their potential security impact on national security, public order, civilians, legal persons, other organisations and public interest in the event of a breach:

- MLPS levels range from Level 1 (low risk) to Level 5 (critical infrastructure)
- core obligations include system registration, risk assessments and implementation of progressively stringent security controls based on classification level
- key technical standards include:
 - Baseline for Classified Protection of Cyber security (GB/T 22239-2019), and
 - Classification Guide for MLPS (GB/T 25070-2019).

Even organisations using outsourced or cloud-based services must ensure MLPS compliance if they build or operate any part of the underlying information systems.

As the MLPS requirements are stipulated in the CSL, failure to comply could result in orders and warnings from the relevant authorities, and fines against the relevant entities and persons directly responsible.

Operational resilience for regulated sectors

Highly regulated sectors, such as finance, healthcare and natural resources, are subject to industry-specific regulations governing a data centre’s capabilities in data recovery, incident response and business continuity.

As an example, subject to:

- the Guidelines on Business Continuity Supervision for Commercial Banks (CBRC Notice [2011] No. 104), and
- the Guiding Opinions on Strengthening IT System Development and Management for Non-Banking Financial Institutions,

financial institutions must establish a **business continuity management system** to ensure rapid recovery of critical operations following disruptions, mitigate or eliminate impacts and losses caused by operational interruptions and safeguard sustained business operations.

Financial institutions must also develop both comprehensive emergency plans and operation specific contingency plans addressing disruption scenarios. Outdated equipment and inadequate risk management measures could result in regulatory penalties.

08. CRITICAL INFRASTRUCTURE AND SECURITY

Critical infrastructure laws

Data centres in China may be designated as CII operators (**CIIOs**) by the relevant authorities, based on factors such as the type and volume of data hosted, industry served and the impact of potential disruption.

There are no specific data type and quantity thresholds issued for the determination of CIIOs. CIIOs are subject to heightened obligations under the CSL, DSL and PIPL. The national standard GB/T 39204-2022 (effective May 2023) outlines criteria for identifying CIIOs and prescribes requirements for security assessments, incident monitoring and emergency response.

National security issues

CIIOs must undergo a cyber security review before procuring any network products or services that may affect national security. Entities handling ‘important data’ under the DSL must comply with extensive obligations. This includes data that could endanger national security, economic stability, social order or public health if compromised.

Obligations include appointing a data security officer and team, implementing data security policies, and regularly conducting risk assessments, monitoring, emergency drills, and training. They must also vet key personnel, manage complaints, and report data disposal plans in scenarios such as dissolution or bankruptcy.

Physical security issues

Data centres are subject to physical security standards, such as:

- GB 50174-2017 – Code for Design of Data Centres, and
- GB/T 51314-2018 - Operation and Maintenance Standard for Data Centre Infrastructure.

The Code for Design of Data Centres classifies facilities into three security levels based on usage, and societal and economic impact. Additional physical security requirements are set out in the Guidelines for the Implementation of Customer Data Security Protection in Internet Data Centres, covering access control, surveillance, and infrastructure integrity.

While not all of these standards are mandatory, they are widely recognised and strongly recommended for compliance and risk management.

09. DATA LOCALISATION

General data localisation requirements

China imposes strict data localisation obligations under the CSL, DSL and PIPL, which outline that:

- CIIOs must store personal data and important data collected within China onshore, unless otherwise specified, and
- cross-border data transfers by CIIOs are only permitted where necessary, do not endanger national security or public interests, and pass a government-led security assessment.

Under PIPL, all data handlers transferring personal data overseas must:

- obtain separate consent from individuals
- conduct a Personal Information Protection Impact Assessment, and
- disclose the purpose, scope and recipient of the transfer.

These rules have led many multinationals (for example, Apple) to host Chinese users' data in local data centres. The regulatory environment continues to drive domestic data centre investment and expansion.



ON THE GROUND

TARGETED OR INDIRECT DATA LOCALISATION REQUIREMENTS

Several industries in China are subject to sector-specific data localisation mandates, even if not expressly labelled as such. These include:

- **Human genetic resources:** Export or access by foreign parties requires prior approval and record-filing with the **Ministry of Science and Technology**
- **Online ride-hailing:** Operators must store **personal and business data** within Mainland China for **at least 2 years**, and cannot transfer it overseas without approval (Interim Measures for the Management of Online Ride-Hailing Services)
- **Internet mapping services:** Map data servers must be located **within China** (Regulations on the Management of Maps), and
- **Online publishing:** Technical infrastructure (servers, storage devices) must be deployed **onshore** (Administrative Provisions on Online Publishing Services).



10. ENVIRONMENTAL, SOCIAL AND GOVERNANCE

International ESG commitments

China was among the earliest signatories and ratifiers of the Paris Agreement (April 22, 2016) and continues to reaffirm its climate commitments through international forums such as COP29.

These commitments have been translated into a broad legal and regulatory framework supporting the country’s green transition. Key instruments include:

- the *Interim Regulations on the Administration of Carbon Emissions Trading* (in force since 2024), which establish the legal foundation for China’s national carbon market
- the *Energy Law of the People’s Republic of China* (adopted in November 2024), which aims to promote high-quality energy development, safeguard national energy security, and support the country’s low-carbon transformation, and
- complementary regulations, such as the *Water Conservation Regulations*, *Ecological Protection and Compensation Regulations*, and *Measures for the Administration of Pollutant Discharge Permits*, further strengthen China’s capacity to regulate environmental impacts across sectors.

ESG laws and standards

China’s green transition is driving a growing set of ESG-related laws and technical standards relevant to data centres, including:

- The *Energy Conservation Act and Renewable Energy Act* providing the foundation for energy efficiency and clean energy integration across industrial operations. While not specific to data centres, it requires high energy users to establish internal energy management policies. Authorities may also supervise and inspect energy usage.
- The *Data Centre Energy Efficiency Limits and Energy Efficiency Grades (GB standard)* establishes mandatory thresholds and grading criteria for energy consumption in data centres.

Policy drivers and spatial planning

China’s ‘*East Data, West Computing*’ initiative is a core ESG-linked strategy that shifts the construction of large-scale data centres toward western provinces. This aims to alleviate pressure on water and energy resources in densely populated eastern cities while making better use of renewable-rich regions inland.

In 2022, the National Development and Reform Commission started construction of national computing hub nodes in 8 regions (Beijing-Tianjin-Hebei, Yangtze River Delta, Guangdong-Hong Kong-Macao Greater Bay Area, Chengdu-Chongqing, Inner Mongolia, Guizhou, Gansu, and Ningxia), and planned 10 national data centre clusters.

The initiative has already delivered notable success, significantly improving the spatial balance of computing resources between eastern and western regions.

11. SECTOR-SPECIFIC REGULATIONS APPLICABLE TO DATA CENTRES

Government bodies

Government procurement of data centre services is subject to strict standards on energy efficiency, environmental protection and data security.

The Green Data Centre Standards mandate technical requirements for government procurement (see [Section 1](#) Power). The *Government Procurement Law* ensures procurement processes are open, transparent and aligned with national priorities.

Telecommunications operators

Participants in the telecommunications sector must comply with procurement-specific rules, such as the *Measures for the Administration of Bidding and Tendering for Telecommunication Engineering Construction Projects*. This governs the construction, reconstruction, expansion and demolition of communication facilities or communication networks, as well as relevant equipment and materials.

Financial services providers or financial institutions

Data centres serving financial institutions are subject to comprehensive IT and operational risk guidelines, covering business continuity, physical security protection and data security.



HONG KONG SAR

CHAPTER 3

SNAPSHOT



As a key financial hub of Asia, Hong Kong is an important data centre market. With 'open door' investment and foreign exchange policies, it stands out as a dynamic centre for technological advancement and investment.

The Hong Kong Government continues to support technology innovation. It has made special development zones available to technology sector players.

Ongoing changes to the US export controls no doubt cast a shadow over the data centre and technology sector in Hong Kong, and it remains to be seen how it will navigate through these uncertainties. That challenge aside, the robust regulatory environment, with its favourable conditions for capital flow and minimal foreign investment restrictions, bolster confidence in Hong Kong's data centre market.

OPPORTUNITIES

- ✓ No FDI, foreign exchange or capital control restrictions
- ✓ Special development zones for the technology sector

CHALLENGES

- ✗ US export controls

SPOTLIGHT ON KEY DRIVERS

EASE OF CAPITAL FLOWS

Hong Kong has always been known for its hands-off 'laissez-faire' economic policies. This creates a free market encouraging businesses to thrive.

With no FDI restrictions, foreign exchange or capital flow restrictions and a stable USD-pegged currency, Hong Kong provides an open market for new data centre investments.

GOVERNMENT SUPPORT

The Hong Kong Government continues to support innovation in the technology sector.

There are a number of special development zones (such as the Hong Kong Science and Technology Park and Hong Kong-Shenzhen Innovation and Technology Park) dedicated to fostering start-ups and innovation in the technology industry. They provide friendly ecosystems which may bring various commercial opportunities to various technology sector players, which may drive the demand for data centre capacity.

US EXPORT CONTROLS

US export controls continue to limit Hong Kong's access to advanced AI chips and technologies, with clear flow on effects for data centre development.

Although the recent rescission of the AI diffusion rule provided some regulatory relief, core hardware-related restrictions remain and are expected to persist. While these controls limit developers' and operators' abilities to source and deploy high-performance computing infrastructure, they also create opportunities for local companies to advance domestic chip development and explore alternative technologies to meet growing data centre demand.

'Hong Kong is a leading destination for data centres in Asia, thanks to its unrivalled connectivity, reliable power and water access, transparent regulatory framework and attractive financing options. Its strategic location and strong business ecosystem offer unique opportunities for clients looking to expand or future-proof their data centre operations in the region.'

Scott Gardiner
Partner
King & Wood Mallesons



OPERATIONAL

01. POWER

Getting power to a site

Power in Hong Kong is supplied through Hong Kong Electric and China Light & Power (**CLP**).

Each utility has its own process. In general, new supply begins with an inspection of the installation to be connected. The timing for completion of new supply will depend on the precise geographical location and existing utility equipment in that location.

Compared with some other jurisdictions such as Japan and Korea, Hong Kong has not experienced the same excessively long lead times for data centre operators to acquire grid connection.



HONG KONG ELECTRIC
Supplying Hong Kong and Lamma Islands



CLP
Supplying Kowloon and the New Territories



BOTH ARE...

vertically integrated utilities operating as monopolies within their respective geographic remits



regulated under Scheme of Control Agreements with the Hong Kong Government (regulating electricity tariffs)

Power purchase agreements

Electricity is supplied on the basis of the general conditions of each of CLP or Hong Kong Electric (depending on location).

CLP and Hong Kong Electric are the only electricity utilities in Hong Kong and there is no alternative to procuring electricity under their general conditions. As a result, corporate PPAs are not permitted.

There is some local solar power generation, mainly small-scale rooftop panels on industrial and residential buildings, as well as private houses. This is used for self-consumption and sale to the relevant utility under a net metering scheme, but space constraints and land pricing are likely to make the use of solar generation a technically challenging option for data centre operators.

02. WATER

Water supply

Water is supplied by the Government's Water Supplies Department. Supply is based on their standard terms and conditions.

Water laws, policies and guidelines

There are no government energy policies that specifically impact the construction and operation of data centres.

03. LAND



WHERE CAN DEVELOPERS BUILD DATA CENTRES?

General zoning requirements apply. Data centres may operate in areas zoned as 'Commercial', 'Industrial' and 'Other Specified Uses' (**OU**) annotated 'Business' (**OU(B)**). In other zones, additional consents may be required.

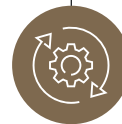
Data centre operators should also confirm if there are any restrictive covenants under the government lease for the target land (most large industrial and commercial buildings are owned under Government leases) and in the deed of mutual covenants (where there are multiple owners) which may restrict or limit the development or operation of a data centre.



ARE ANY PERMITS OR APPROVALS REQUIRED?

No specific permits or land-related approvals are required to develop, construct or operate data centres.

If there are restrictive covenants in the government lease which may materially impact the development and operation of a data centre, a lease modification or a waiver may be required to develop a data centre.



WHAT IF RE-ZONING OR CHANGES TO COVENANTS ARE NEEDED?

Applications for re-zoning must be made to the Town Planning Board. The Town Planning Board is required to hold a meeting with the applicant to consider the application within 2 months of receiving the application. However, the timeframe for making the final decision is more fluid.

Applications to change or relax restrictive covenants under the Government lease must be made to the Lands Department. There are no clear timelines for applicants to change the terms of the Government lease and some applications can take several years.



04. TELECOMMUNICATIONS

Is a telecommunications licence required?

A telecommunications licence is not ordinarily required to operate a data centre, where the operator is simply providing rack space, or processing capacity in a data centre. However, a data centre operator may need a licence if it:

- provides telecommunications services at or to the facility, or
- operates certain types of specialised telecommunications equipment requiring a licence.

A list of telecommunications services that require licensing is available on the [website of the Communications Authority](#).

Applicability of telecommunications laws to data centres

Data centre developers and operators are not subject to telecommunications regulations in Hong Kong, unless they provide telecommunications services or operate equipment requiring a licence (see above).



STRATEGIC OPPORTUNITIES



05. FOREIGN INVESTMENT RESTRICTIONS

There are no material foreign investment restrictions in Hong Kong.

06. TAX AND OTHER INCENTIVES

Special economic zones

The Hong Kong Government has proposed a new development that is intended to grow into an international centre for innovation and technology. Known as the [Northern Metropolis](#) and integrating with nearby Shenzhen, it includes a technology hub, San Tin Technopole.

Cyberport, Hong Kong Science and Technology Park and Hong Kong-Shenzhen Innovation and Technology Park are examples of thematic development areas within the Northern Metropolis. Due to Hong Kong's low taxation and convertibility of capital, the tax incentives provided by these locations are more limited than in other jurisdictions, but they also offer various grants, subsidies and incubator programmes (not necessarily specifically targeted at data centres).

‘LOCATED AT THE HEART OF THE NORTHERN METROPOLIS AND IN CLOSE PROXIMITY TO SHENZHEN'S INNOVATION AND TECHNOLOGY (I&T) ZONE IN HUANGANG AND FUTIAN, SAN TIN TECHNOPOLE WILL BECOME A HUB FOR CLUSTERED I&T DEVELOPMENT THAT CREATES SYNERGY WITH SHENZHEN I&T ZONE.’
NORTHERN METROPOLIS

Tax incentives and other incentives

There are generally no available tax incentives for operators, developers or owners of data centres. However, the Hong Kong Government has indicated it is open to considering, on a case-by-case basis, waivers of onerous or restrictive covenants in government leases (under which most of the land relevant to data centre developers is held) to facilitate the development of data centres.

COMPLIANCE AND RISK MANAGEMENT

07. DATA PROTECTION AND CYBER SECURITY

Data protection or privacy laws

A general framework for the collection, processing and protection of personal data is in the *Personal Data (Privacy) Ordinance (PDPO)*. The PDPO primarily regulates data users who control the collection, holding and processing of personal data.

Data users are required to ensure that their **data processors** (that is, persons who process personal data on behalf of a data user and not for its own purposes) comply with certain regulatory requirements such as data security. Practically, these regulatory requirements are more likely to apply to customers of data centre operators rather than the operators themselves.

08. CRITICAL INFRASTRUCTURE AND SECURITY

Critical infrastructure laws

A new range of organisational, preventative, monitoring and reporting obligations on operators of critical infrastructure, with a view to minimising cyberattacks, is expected to take effect on 1 January 2026.

The Protection of Critical Infrastructure (Computer System) Bill (**Critical Infrastructure Bill**) was passed on 19 March 2025.

The Critical Infrastructure Bill defines ‘critical infrastructure’ to mean:

- any infrastructure that is essential to the continuous provision in Hong Kong of an **essential service** in 8 specified sectors, including, relevantly:
 - energy
 - information technology
 - banking and financing services
 - telecommunications, and
 - broadcasting services, or
- any other infrastructure, the damage, loss of functionality or data leakage of which, may hinder or otherwise substantially affect the maintenance of **critical societal or economic activities** in Hong Kong.

The definition is broad enough to capture data centres, depending on their customer base and use.

National security issues

National security matters are regulated by the *Law of the PRC on Safeguarding National Security in the HKSAR (National Security Law)* and *Instrument A305 Safeguarding National Security Ordinance (Instrument A305)*. These regulations impose various criminal sanctions against a wide range of offences relating to national security. They are not specific to data centres but are of general application. However, section 50 of Instrument A305 expressly criminalises actions in relation to a computer or electronic system which endangers, or is likely to endanger, national security.

09. DATA LOCALISATION

In general, there are no data localisation or residency requirements in Hong Kong. However, see [Section 11](#) Sector-specific regulations for requirements relating to government bodies, digital asset providers and stablecoins.

10. ENVIRONMENTAL, SOCIAL AND GOVERNANCE

International ESG commitments

The government of China has decided that the Paris Agreement applies to Hong Kong.

Key ESG laws, regulations and guidelines

There is no specific statute relating to implementation of the Paris Agreement, but the Hong Kong Government has issued schemes and plans.

- The Buildings Department has issued several practice notes and guides including the **Green Data Centres Practice Guide**.
- The **Climate Action Plan 2050** - sets decarbonisation targets for electricity, transport, buildings and waste.
- The **Building Energy Efficiency Ordinance**:
 - applies to a wide range of building types (including industrial and commercial buildings)
 - imposes energy efficiency standards on the design of new buildings (or existing buildings undertaking major retrofitting works).
- The **Fresh Water-Cooling Towers Scheme** is a voluntary government scheme that sets standards for the design, installation, operation and maintenance of water-cooling towers.

ESG reporting

ESG reporting only applies to companies listed on the Hong Kong Stock Exchange, which are required to report on their ESG performance against set KPIs, based on a ‘comply or explain’ system. There are currently no ESG reporting requirements which are specifically targeted at the data centre sector.

BEAM Plus

The Hong Kong Green Building Council has been promulgating the use of the BEAM Plus standards for new buildings in Hong Kong, which include a number of energy efficiency and sustainability standards for the design, construction and operation of buildings.

Buildings meeting the BEAM Plus standards (which set out different ratings based a building’s environmental footprint) can apply to be certified by the Hong Kong Green Building Council. It is becoming increasingly common for construction contracts in Hong Kong to require buildings to receive BEAM Plus certification. Note that BEAM Plus standards apply generally to all buildings and there are no specific standards applicable to data centres.

AS ONE OF THE WORLD’S BIGGEST FINANCIAL HUBS, HONG KONG IS DECARBONISING ITS ECONOMY BY PLAYING TO ITS STRENGTHS: FINANCE AND TECHNOLOGY. FIND OUT HOW THESE ‘DUAL ENGINES’ ARE POWERING TRANSFORMATION – AND WHAT IT MEANS FOR BUSINESSES.



11. SECTOR-SPECIFIC REGULATIONS APPLICABLE TO DATA CENTRES

Government bodies





The Hong Kong Government has its own policies in relation to IT security (Government Information Technology Security Policy and Guidelines), some of which deal with data centres. They are mostly relevant to data centre operators providing services to the Hong Kong Government.

Specifically, the Government must ensure that data centres:

- have good physical security and strong protection from disaster and security threats
- comply with the relevant government requirements on physical security, and
- monitor all visitors and keep active records of visitor access.

Financial services providers or financial institutions

The major financial services providers that have specific rules or guidelines on the use of data centres and data centre services are:

 01 LICENSED CORPORATIONS	 02 AUTHORISED INSTITUTIONS (THAT IS, BANKS)	 03 STORED VALUE FACILITIES (SVF) LICENSEES	 04 AUTHORISED INSURERS
Licensed by the Securities and Futures Commission of Hong Kong (SFC) Regulated by the Securities and Futures Ordinance (Cap. 571 of the Laws of Hong Kong) and other circulars and FAQs published by the SFC	Licensed by the Hong Kong Monetary Authority (HKMA) Regulated by the Banking Ordinance (Cap. 155 of the Laws of Hong Kong) and Supervisory Policy Manuals	Licensed by the HKMA Regulated by the Payment Systems and Stored Value Facilities Ordinance (Cap. 584 of the Laws of Hong Kong) and the Guideline on Supervision of Stored Value Facility Licensees	Licensed by the Insurance Authority of Hong Kong Guided by the Guideline on Cyber security and the Cyber Resilience Assessment Framework

For each of these financial services providers, the different laws or regulatory guidelines govern the parameters for the use of data centres and their services. As a general point, regulatory guidelines published by regulators are not strictly mandatory, but failure to comply with them may have adverse impact on the financial service provider (for example, disciplinary action, or a revocation of licence in the worst-case scenario).



Digital asset providers

Virtual asset trading platform (VATP) operators, such as virtual assets exchanges, licensed by the SFC are expected to follow:

- the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap. 615 of the Laws of Hong Kong)
- the Guidelines for Virtual Asset Trading Platform Operators, and
- other circulars and FAQs published by the SFC.

These require VATP operators to obtain **prior written approval** from the SFC before they can keep regulatory records with an external electronic data storage provider and impose various data security requirements relating to offsite data storage. This includes back-up and contingency planning requirements.

Stablecoins regime

The Stablecoins Bill was passed in May 2025 by the Legislative Council of Hong Kong and the *Stablecoins Ordinance* (Cap. 656 of the Laws of Hong Kong) is expected to come into effect on 1 August 2025. The Financial Services and Treasury Bureau, the HKMA and the SFC are separately working on the regulatory requirements relating to the supervision and custody of digital assets such as stablecoins.

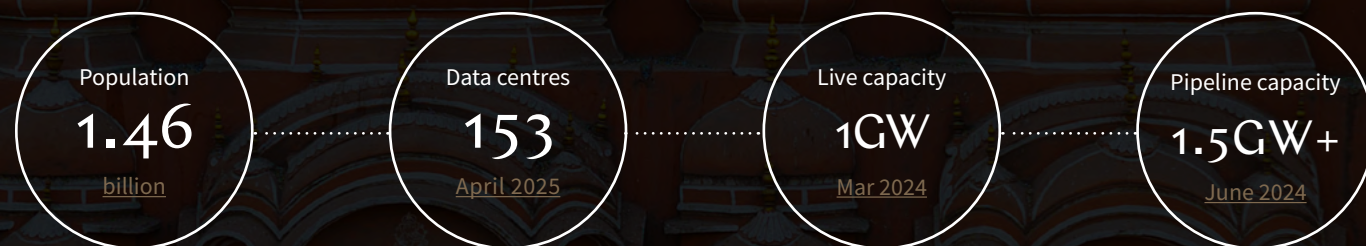
We expect there will be granular requirements in relation to the physical location of private keys and other records, which may impact data centre operators providing services to regulated entities under the Stablecoins Ordinance.

In this guide, references to ‘Hong Kong’ are references to the Hong Kong Special Administrative Region of the People’s Republic of China.

INDIA

CHAPTER 4

SNAPSHOT



India's data centre industry is experiencing rapid growth. Capacity is expected to reach 1.8GW by 2027, driven by digital transformation, favourable government policies and AI adoption.

For investors and operators, the market presents significant opportunities, including access to a large and growing customer base, tax and infrastructure incentives offered by various states and increasing localisation requirements across regulated sectors.

Challenges remain - particularly around land acquisition, regulatory complexity across jurisdictions, evolving data protection laws and compliance with sector-specific obligations. Navigating these hurdles effectively is essential to capitalise on India's strong long-term growth potential in the data centre sector.

OPPORTUNITIES

- ✓ Increasing onshore demand for data storage from local entities
- ✓ Government incentives
- ✓ Renewable energy incentives

CHALLENGES

- ✗ Fragmented land and zoning regulations
- ✗ Evolving regulatory landscape

SPOTLIGHT ON KEY DRIVERS

A SHIFT TO SELF-GENERATION OF POWER AND RENEWABLES

India's regulatory landscape is increasingly supportive of renewable energy use within the data centre sector.

Several Indian states offer exemptions or concessions on electricity duties and transmission charges to incentivise adoption. As a result, data centre operators are investing in captive solar and wind projects to ensure a more stable and cost-effective power supply. These initiatives also help operators navigate grid constraints and reduce dependence on state utilities. The ability to self-generate power is becoming a key strategic consideration in site selection and long-term infrastructure planning.

GOING 'GREEN'

More Indian states are introducing supportive measures. With global demand for sustainable and green energy on the rise, improved access to affordable renewables will enhance India's attractiveness as a data centre hub.

Several state-level policies actively incentivise this shift. For example, Odisha's 2022 data centre policy offers reimbursement of transmission and wheeling charges for power drawn from captive renewable sources. While there are no legal mandates requiring the use of green energy, the regulatory environment strongly encourages it. Coupled with growing pressure from customers and investors to meet global ESG standards, these measures are positioning India as a compelling destination for sustainable data centre investment.

MATURING TELCO AND DATA REGULATORY LANDSCAPE

India's regulatory landscape for data centres is set for major change.

These regulatory changes may present new compliance challenges, but they may also drive demand for onshore data storage solutions and create new growth opportunities in the sector.

- The scope of 'telecommunication services' is expected to broaden under the *Telecommunications Act 2023 (Telco Act)*, potentially including colocation services (which traditionally sit outside telecom regulation), imposing new licensing and compliance obligations. This won't be confirmed until the delegated legislation is released.
- The hotly anticipated *Digital Personal Data Protection Law 2023 (DPDP Law)* will introduce new data protection requirements across the board.
- Targeted data localisation requirements in sectors like financial services and telecommunications are prompting companies to expand local storage capacity.

'India's data centre industry is experiencing strong growth due to digital demand, cloud adoption and government incentives. Although the regulatory framework is still fragmented, recent laws are improving compliance, especially regarding data sovereignty and user privacy. Cloud service providers and new entrants should prepare for clearer regulations focusing on local data storage and cybersecurity. Aligning with these trends will give operators a long-term advantage in a formalising market.'

Jishnu Sanyal
Partner
Trilegal



OPERATIONAL

01. POWER

Getting power to a site

Data centres are entitled to request a power connection from the local distribution company (**DisCom**) under the *Electricity Act 2003 (Electricity Act)*.

The DisCom **cannot refuse supply** - even where grid extension or augmentation is required.

Upon approval, the DisCom typically **installs a meter** and enters into a supply agreement with the consumer, or grants connection based on state-specific supply codes issued by the State Electricity Regulatory Commission (**SERC**).

DisComs are ordinarily required to begin supplying power **within 1 month of application**, though this may be extended depending on grid readiness and site-specific factors.

Before supply begins, the DisCom conducts a **60 to 90 day feasibility study** to assess grid capacity and reach. Timelines vary by state and depend on site location, grid availability and power purchase arrangements (**PPAs**). Interstate power procurement requires additional approvals, typically taking 6 to 8 months.

Power purchase agreements

Developers can procure electricity under corporate PPAs with independent electricity suppliers. In the past few years, these suppliers have been able to, in some cases, offer:

- **lower tariffs** than DisComs, and
- **more favourable contractual terms**, such as termination or compensation rights if PPA tariffs exceed those of the local DisCom.

Corporate PPAs can take the form of onsite physical PPAs (generation assets are located on the premises of the end user/purchaser) or offsite physical PPAs.

Corporate offsite physical PPAs leverage the non-discriminatory open access regime provided under the Electricity Act. This allows purchasers to use DisCom or transmission licensee networks to procure power from third-party suppliers outside their local DisCom. To implement open access, each state has its own regulations, procedures and standard agreements covering aspects such as wheeling, banking and grid connectivity.

AS THESE REQUIREMENTS VARY BY STATE, DATA CENTRE OPERATORS MUST CAREFULLY NAVIGATE THE SPECIFIC RULES IN THE STATE WHERE THEY INTEND TO PROCURE RENEWABLE ENERGY.

Inter-state corporate physical PPAs are also possible and have been implemented at utility scale. For example, Amazon’s corporate PPA with CleanMax’s inter-state grid for the development of a 100MW wind power project in Karnataka. However, they are subject to additional regulatory and physical constraints compared to intra-state corporate physical PPAs.

Corporate virtual PPAs are possible, although generators and buyers should note that they may be considered as ‘commodity derivatives’ regulated by the Securities Exchange Board of India, possibly subjecting them to licensing, reporting and compliance requirements.

Going ‘green’

Data centres may opt for green energy open access when sourcing renewable power from a generator within the same state. If the generator has available capacity, operators can apply through the **designated nodal agency, which must respond within 15 days** - failing which, approval is deemed granted, subject to technical clearance by the relevant SERC.

While there are no laws mandating the use of a specific power source for data centres, several state-level data centre policies actively incentivise renewable energy adoption.

Odisha’s State Data Centre Policy of 2022, for example, offers reimbursement of transmission and wheeling charges for power drawn from captive renewable plants. With India’s dual focus on promoting data centre infrastructure and clean energy, more states are expected to introduce similar incentives.

02. WATER

Water supply and infrastructure

Water supply is regulated at both central and state levels.

Designated special zones, known as ‘data centre parks’ or ‘data centre campuses’, for data centre development exist in some states and come pre-equipped with core infrastructure. Some also include shared water and sewage treatment facilities, while others permit developers to build their own.

Data centre parks and data centre campuses

Located in states like Maharashtra, Karnataka, Haryana, Gujarat and Telangana.

Sites feature core infrastructure, including:

- continuous water supply for cooling systems, and
- water and sewage treatment facilities or permission for developers to build their own.

Regulation of groundwater use

Groundwater use is regulated under the *Environment Protection Act 1986*. Data centre operators must obtain a **no-objection certificate** from the Central Ground Water Authority or relevant state authority to extract groundwater.



03. LAND



04. TELECOMMUNICATIONS

Starting a data centre business - is a telecommunications licence required?

Only if the data centre operator or developer establishes its own telecom links between sites.

Otherwise, data centre developers and operators in India are currently not required to hold a telecom licence, as they are not considered telecom service providers under the *Indian Telegraph Act 1885* (**Telegraph Act**).

This position may change under the new Telco Act, which is currently being implemented in stages to replace the existing telecommunications legislation. The Telco Act proposes:

- a broader definition of ‘telecommunication services’ that **could extend to colocation services**, and
- a wide definition of ‘telecommunication network’ that **may include active infrastructure such as routers, switches, servers, load balancers and passive infrastructure** such as racks, power and cooling systems if they are deemed to form a telecommunication network.

Applicability of telecommunications laws to data centres

As a result, new licensing or compliance obligations may apply to data centre operators, even if they do not own telecom links between sites. That said, the precise scope and impact remains uncertain until the delegated legislation is released.

Data centre developers and operators are not directly regulated under Indian telecommunications laws. However, under the Telegraph Act government agencies can direct telecom service providers (**TSPs**) to **monitor or intercept data centre traffic** which, while will not directly impact data centre operators, may indirectly affect them through their dealings with TSPs.

STRATEGIC OPPORTUNITIES

05. FOREIGN INVESTMENT RESTRICTIONS

Land

In India, foreign investment is governed by *Foreign Exchange Management (Non-debt Instruments) Rules 2019* (**Non-Debt Rules**) notified under the *Foreign Exchange Management Act 1999* (**FEMA**).

Foreign entities generally cannot acquire immovable property directly unless they establish a local presence, such as a liaison office, branch, subsidiary under the *Companies Act, 2013* (**Companies Act**), or a limited liability partnership(see [Section 3](#) Land above).

Even then, they are prohibited from acquiring agricultural or plantation land, unless it is first converted to non-agricultural use. While FDI in ‘real estate business’ (dealing in land or immovable property for profit) is prohibited, **this restriction does not apply to infrastructure development**, including data centres.

As such, FDI is permitted for land acquisition for data centre development, provided the investment is not for speculative purposes and does not fall within the prohibited definition of ‘real estate business’.

Data centres

The only restriction is for investments where the beneficial owner is situated in, or is a citizen of **any countries sharing a land border** with India.

These are China, Bangladesh, Pakistan, Bhutan, Nepal, Myanmar and Afghanistan (each is a **Restricted Country**).

Investments from those in Restricted Countries require prior approval of the Indian government.

Telecommunications

India generally permits **up to 100% FDI** in sectors like telecommunications, broadcasting, manufacturing and infrastructure under the *Foreign Exchange Management (Non-debt Instruments) Rules 2019*. However, FDI from Restricted Countries requires prior government approval.

06. TAX AND OTHER INCENTIVES

Special economic zones

India has established several SEZs to attract investment and promote the export of services, including data centres. These SEZs offer a tax-efficient environment with incentives such as duty-free procurement of goods and services.

Notable SEZs relevant to data centres include Maharashtra, Karnataka, Tamil Nadu and Uttar Pradesh, offering tax exemptions and infrastructural support to the business units, including data centres, set up within them.

Tax incentives

Various states in India offer tax incentives to encourage data centre development. For instance, Maharashtra provides fiscal incentives like stamp duty and electricity duty exemptions for data centres meeting certain eligibility criteria.

These benefits apply beyond SEZs and form part of broader state-level investment policies. Maharashtra has seen significant investment, including Yotta Infrastructure’s large-scale facility.

Other incentives

In addition to tax incentives, states offer non-fiscal benefits such as assured power supply, land allocation and infrastructure support. These are typically provided under dedicated data centre policies, separate from SEZ schemes, though some overlap may occur.

Several states have set up data centre parks with ready infrastructure, making them more attractive for investment.

The central government is also developing a national data centre policy to further streamline and coordinate these incentives.



COMPLIANCE AND RISK MANAGEMENT

07. DATA PROTECTION AND CYBER SECURITY

Data protection or privacy laws

India’s data protection laws apply to **all entities processing personal data**, and do not distinguish between data centres and data centre services.

Under the *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SDPI Rules)*, obligations are minimal and focus on maintaining reasonable security standards, such as ISO 27001.

Data centres acting **solely as data processors** under contractual arrangements **are exempt** from certain requirements, such as obtaining user consent or providing access or correction rights.

The upcoming DPDP Law introduces broader obligations for entities controlling personal data (data fiduciaries), including implementing reasonable security safeguards. While primary compliance lies with data fiduciaries, these obligations are often contractually passed on to data processors, including data centres.

Cyber security laws

Data centres and service providers in India are subject to cyber security rules issued by the Indian Computer Emergency Response Team (**CERT-In**) under the *Information Technology Act 2000 (IT Act)*. These obligations apply uniformly to data centres, cloud providers and intermediaries, without distinction between infrastructure and services.

Key cyber security requirements include:

- mandatory reporting of specified cyber incidents **within 6 hours** of becoming aware
- retention of **ICT system logs** in India for **180 days**
- customer **information retention for 5 years**, including validated identity and contact details, IP allocation, timestamps, purpose of service and ownership details, and
- **clock synchronisation** with authorised Indian Network Time Protocol servers.

08. CRITICAL INFRASTRUCTURE AND SECURITY

Critical infrastructure laws

Data centres are classified as ‘computer resources’ under the IT Act and are not generally classified as Critical infrastructure. However, they may be designated by the government as ‘protected systems’ if they are linked to Critical infrastructure. That is, to systems whose failure would severely impact national security, the economy, public health or safety. Key sectors include energy, banking, telecom, transport and healthcare.

The government **may designate specific data centres as protected systems** based on factors such as national security, economic impact, public safety and interdependence with other critical infrastructure, under Section 70 of the IT Act. Designated data centres must comply with **strict security protocols**, including the establishment of cyber security and network operations centres.

National security issues

Government agencies are authorised to **monitor or intercept data** transmitted through data centres if it affects national security, under the IT Act. Certain agencies, such as the CERT-In, may direct data centres to provide online access to their systems to monitor traffic and collect data. These requests are typically aimed at enhancing cyber security and preventing the spread of malware or other threats.

09. DATA LOCALISATION

No general data localisation requirement

India does not impose general data localisation requirements. Both the SDPI Rules and the upcoming DPDP Law allow cross-border data transfers, subject to certain conditions, but do not mandate general data localisation.

Targeted or indirect data localisation requirements

Sector-specific requirements are enforced across regulated industries. These affect **where and how** data – particularly sensitive or regulatory data – must be **stored and processed**.

THESE SECTOR-SPECIFIC DATA LOCALISATION RULES MAY BE CONTRIBUTING TO INCREASED INVESTMENT IN INDIAN DATA CENTRES, AS COMPANIES EXPAND ONSHORE STORAGE TO SUPPORT COMPLIANCE EFFORTS.

It’s important to note that certain sector-specific localisation restrictions are currently in place (more on this below).

- **Financial services:** The Reserve Bank of India (**RBI**) imposes multiple localisation mandates for entities it regulates, including banks and payment system providers. For example:
 - all **data and recordings** from video-based customer identification must be exclusively stored in India under KYC rules
 - payment system providers must store end-to-end **transaction data** within India. Processing abroad is permitted, but data must return to India within 24 hours, and
 - regulated entities **outsourcing IT services** must ensure all related data is stored in India.

- **Securities:** The Securities and Exchange Board of India requires certain intermediaries using SaaS-based solutions to store critical operational data in India. This includes risk-related data (credit, liquidity, market), internal network and design information, audit data and supplier data.
- **Insurance:** The Insurance Regulatory and Development Authority of India requires all insurers to store original policyholder records, including electronic records, within data centres located in India.
- **Telecoms:** Licensed telecom service providers must store subscriber data, accounting information, network logs, and IP records within India, and are generally prohibited from transferring this data overseas except in limited cases like international roaming or legal requirements.

Additionally, all data centres, service providers, intermediaries, government bodies and corporates must **retain secure copies of IT system logs** in India for at least **180 days**, though storage need not be exclusive to India.

However, changes are on the horizon. The Draft Rules under the DPDP Law propose localisation requirements for entities designated as significant data fiduciaries, restricting cross-border transfer of certain personal and traffic data.

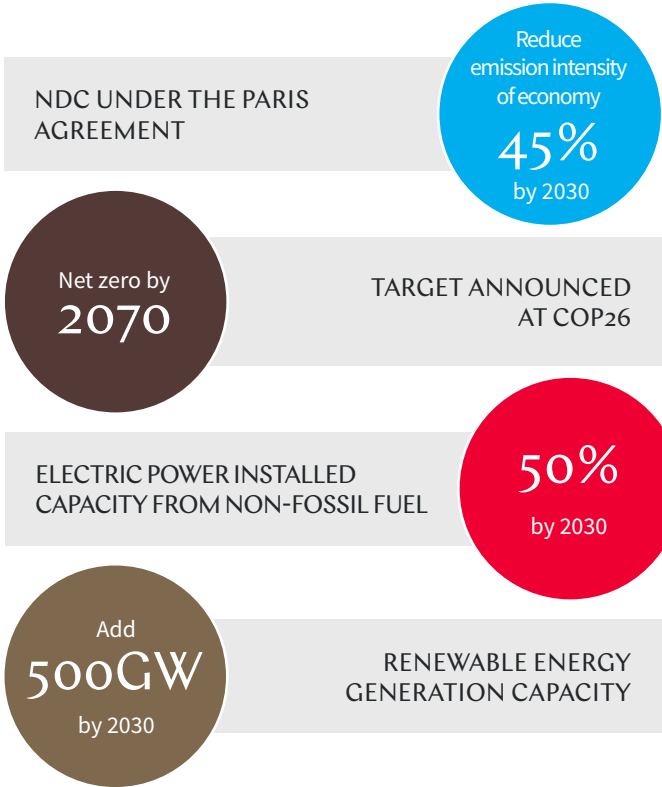
While the existing telecommunications data localisation requirements remain in place, new rules under the incoming Telco Act may also revise data localisation obligations in the telecom sector, which may affect data centres.



10. ENVIRONMENTAL, SOCIAL AND GOVERNANCE

International ESG commitments

India ratified the Kyoto Protocol in August 2002 and the Paris Agreement in October 2016. In line with its commitments under the Paris Agreement, India updated its NDCs in 2022.



Environmental requirements

Data centres in India are classified as ‘communication’ sector infrastructure, and generally subject to laws and regulations applicable to infrastructure projects.

While a Draft Data Centre Policy, released in 2020, proposed a single-window clearance system, it remains unfinalised and silent on specific permit requirements. In practice, ESG compliance for data centres is shaped by a combination of central and state-level frameworks.

On environmental impact, data centres:

- must comply with the *Environment Protection Act 1986*, and
- may require environmental clearance under the EIA Notification 2006, as well as consent from State Pollution Control Boards under the *Air (Prevention and Control of Pollution) Act 1981*, and *Water (Prevention and Control of Pollution) Act 1974*, if they are likely to discharge pollutants.

ESG reporting

There are no ESG reporting requirements specific to data centres. However, data centre owners or operators may be required to disclose ESG data under broader frameworks, such as Securities and Exchange Board of India’s mandatory reporting of ESG data (including carbon emissions) for the top 1,000 listed companies.



11. SECTOR-SPECIFIC REGULATIONS APPLICABLE TO DATA CENTRES

Government bodies

Data centres serving Indian government bodies must comply with specific operational and security standards. Under the Meghraj initiative, cloud providers seeking empanelment must:

- host data within India
- obtain ISO certifications (27001, 27017, 27018), and
- undergo audits by the Standardisation Testing and Quality Certification Directorate to verify compliance.

Financial services providers or financial institutions

RBI-regulated entities outsourcing IT services, including to data centres, must comply with the Master Directions on Outsourcing of IT Services. Key requirements include:

- implementing an IT outsourcing policy
- conducting risk-based due diligence
- signing agreements with prescribed clauses
- maintaining a risk management framework
- monitoring outsourced activities, and
- ensuring service providers report cyber incidents promptly so the entity can meet a 6 hour RBI reporting deadline.

Digital certification bodies

Certifying Authorities licensed under the IT Act must follow specific rules when engaging third-party service providers, including data centres, under the *Information Technology (Certifying Authorities) Rules, 2000* when engaging third-party service providers such as data centres. Key requirements include:

- limiting and securing external network connections to essential functions only
- conducting risk assessments before outsourcing services
- ensuring infrastructure is located in India
- having outsourcing agreements approved by the relevant information asset owner, and
- requiring service providers to implement security controls and sign non-disclosure agreements.



INDONESIA

CHAPTER 5

SNAPSHOT



Indonesia is one to watch in the APAC region for data centre growth. The draw of tax incentives and special economic zones, coupled with low barriers to foreign investment, has made it an attractive destination for investment from big global players.

Tencent Cloud, to give one prominent example, has pledged to funnel US\$500 million into infrastructure in Indonesia by 2030. Its third data centre in the country became fully operational in June 2025, in what it celebrated as 'one of the largest and most complex cloud relocations ever undertaken in Southeast Asia'.

Rapid growth presents challenges, but the Indonesian government and industry leaders are collaborating on solutions. The government's digital infrastructure push aligns with Indonesia Emas 2045 (or 'Golden Indonesia'), its vision for a prosperous and advanced nation by 2045.

As Indonesia transforms into a hub for data centres, it is poised to drive economic growth and technological advancement.

OPPORTUNITIES

- ✓ Fiscal and non-fiscal incentives
- ✓ Minimal obstacles to foreign investment

CHALLENGES

- ✗ Restricted options for procuring power and water supply
- ✗ Disparity in infrastructure quality across regions

SPOTLIGHT ON KEY DRIVERS

IN THE ZONE

Indonesia requires data centres to be located in designated industrial estates, which are supported by essential infrastructure for power and water.

This is helpful, with the quality of infrastructure varying widely across the country. Location exemptions are available in certain circumstances, but this general location restriction nonetheless limits site selection flexibility. Data centre businesses can receive a number of fiscal and non-fiscal incentives in SEZs established by the Indonesian government to promote investment in various industries. These foster economic growth and technological advancement.

RENEWABLE FUTURES

Indonesia's commitment to renewable energy and sustainability broadly, as a signatory to the Paris Agreement, represents a forward-looking driver for the sector.

Although not yet fully codified in regulations specific to data centres, this encourages operators to invest in sustainable practices, aligning with global trends.

'In the past five years Indonesia has dramatically evolved into a top destination for digital infrastructure. We've seen investments surge, driven by major players.'



Ayik Candrawulan Gunadi
Partner
Ali Budiardjo Nugroho Reksodiputro

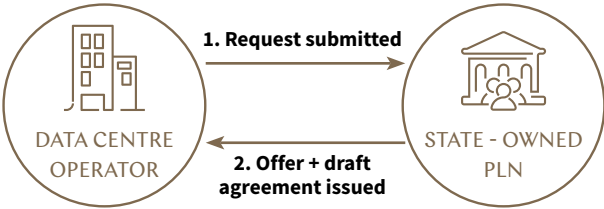
OPERATIONAL

01. POWER

Getting power to a site

Indonesia’s state-owned company, Perusahaan Listrik Negara (**PLN**), is the primary supplier of electricity under a quasi-monopoly. Private participation in electricity supply business activities is permitted, but only in certain areas and with government approval. To secure power from PLN for a data centre site, a request must be submitted to PLN, which they will then issue an offer and a draft agreement.

The lead time in the power procurement process is highly variable and depends heavily on PLN's capacity and infrastructure availability at the location. PLN infrastructure varies between regions, so not all locations are able to provide the stable high-load electricity required by data centre.



Typically direct PPA
PLN's Standard terms
Green power - only via onsite PPA

Power purchase agreements

Direct PPAs with PLN are typical for large end users like data centres.

These are usually **executed directly** between data centre operators and PLN, with the agreement based on PLN's standard PPA terms.

When it comes to **green power**, corporate offsite physical PPAs and corporate virtual PPAs are not permitted in Indonesia, but corporate onsite physical PPAs are possible via operational lease arrangements.

In essence, the power plant owner leases the plant to the consumer on economic terms that mimic a conventional PPA for the consumer's use of the power. Excess may also be sold to a licensed energy business. Such operational lease arrangements for green power are common for solar power plants.

Data centre power regulations are expected

There are currently no laws or guidelines regarding the source of power for data centres. However, the government is **currently drafting regulations governing the infrastructure** of data centres. These are expected to cover matters such as:

- networks
- security
- detection
- electricity
- architecture
- ventilation management, and
- operational standards.

The government has not yet issued any of the mandatory standards for data centres, nor is there any indication of when the relevant regulations will be announced or published.



General conservation requirements

All businesses in Indonesia that use energy in an amount greater than or equal to the equivalent of 4,000 tonnes of oil are required under *Government Regulation No. 33 of 2023 on Energy Conservation* (GR 33/2023) to adopt certain energy conservation management practices, including:

- electing an energy manager
- drafting an energy efficiency program
- implementing regular energy audits, and
- implementing recommended energy conservation measures.

The role of renewables

Renewable energy is anticipated to play a significant role in powering data centres, as indicated by statements from PLN's leadership.

'I BELIEVE THAT INDONESIA'S AMBITION IS TO BALANCE ECONOMIC PROGRESS WITH ENVIRONMENTAL SUSTAINABILITY THROUGH ENERGY TRANSFORMATION. WITH ROBUST COLLABORATION, WE ARE CONFIDENT THAT INDONESIA WILL LEAD THE CLEAN ENERGY TRANSITION IN THE REGION.'

02. WATER

Water supply

The procurement and provision of water to data centres is governed by *Law No. 17 of 2019 on Water Resources* (**Water Law**).

Framework for water supply

Approved suppliers from whom businesses in Indonesia must obtain water supply include:

- STATE-OWNED ENTERPRISES
(*BADAN USAHA MILIK NEGARA OR BUMN*)
- REGIONAL-OWNED ENTERPRISES
(*BADAN USAHA MILIK DAERAH OR BUMD*)
- APPROVED PRIVATE ENTITIES

All water resources are explicitly reserved for state control to be used for the **benefit of the broader community** for daily consumption.

According to the Water Law, the use of water resources for the businesses purposes is only permitted upon obtaining government-issued permits and subject to the water management fees charged by the approved suppliers.

There is a statutory hierarchy of priority for the granting of water use permits, for which **commercial business purposes of non- state entities is the lowest priority level (of 5)**, after higher-priority items such as public drinking water, agriculture and irrigation. Permits will only be granted for commercial use after all higher priority matters have been addressed.

ACCORDINGLY, THE TIMELINE FOR PROCURING WATER SUPPLY FOR HIGH-DEMAND ACTIVITIES SUCH DATA CENTRES DEPENDS ON THE AVAILABILITY OF RESOURCES AND INFRASTRUCTURE AS WELL AS THE COMPETING NON-COMMERCIAL WATER DEMANDS IN THE RELEVANT LOCATION.



03. LAND

Where to build

Data centre operations – including hosting activities, data processing services and cloud computing services – are governed by the Standard Industrial Business Code (*Kode Baku Lapangan Industri or KBLI*) 63112, under the *Ministry of Industry Regulation No. 9 of 2021*. Any business undertakings covered by the Code can only operate in industrial estates (*Kawasan Industri*) specifically established by the government.

THERE ARE OVER 100 INDUSTRIAL ESTATES ESTABLISHED ACROSS INDONESIA, WITH MOST OF THEM LOCATED ON JAVA ISLAND. THIS IS A REQUIREMENT OF MINISTER OF INDUSTRY REGULATION NO. 1 OF 2020 ON THE PREPARATION OF A DETAILED RKL-RPL FOR INDUSTRIAL COMPANIES THAT ARE OR WILL BE LOCATED IN AN INDUSTRIAL AREA.

Rezoning areas

Private entities or individuals may submit proposals to rezone certain areas into industrial estates. *Government Regulation No. 20 of 2024 on the Industrial Regionalisation* stipulates that discretion to designate land as industrial estates rests with the Industrial Estate Committee. Its members include representatives from the central Indonesian government and industrial estate associations. This process can be lengthy, and outcomes are dependent on political factors and physical characteristics of the land.

Operating beyond Industrial Estates

Data centre operators may also seek an exemption from the Ministry of Industry to operate a data centre outside an industrial estate under certain conditions, including a lack of available industrial estates or special location or resource requirements. Anecdotaly, the Ministry **tends to take a flexible approach** to such exemptions.



Permitting and approvals

Constructing a data centre requires compliance with general building regulations rather than data centre-specific permits. Key approvals include:

- a Building Construction Permit (*Persetujuan Bangunan Gedung* or **PBG**) before commencing construction, and
- a Certificate of Functional Worthiness (*Sertifikat Laik Fungsi* or **SLF**) after the building is constructed but before its use, confirming adherence to the PBG.

The timeframe for securing these permits varies based on regional government processes and infrastructure readiness.

04. TELECOMMUNICATIONS

When is a licence required?

If a data centre operator intends to offer telecommunications services, such as internet connectivity, as an add-on or as part of a bundle with colocation services, or if it operates an internal telecommunications network, it must obtain a telecommunications operation licence.

However, data centres that **merely offer colocation services and procure connectivity** to the data centre from licensed ISPs are not considered telecommunications service providers and **do not require a licence**. As an example, this would involve constructing a connection point within the data centre site, such that the tenants procure internet connectivity from the ISP directly and link their equipment within the data centre to the ISP's connection point.

In certain circumstances, pursuant to the *MOCD Regulation No. 12 of 2018 on the Provision of Special Telecommunications for the Needs of Government Agencies or Legal Entities*, data centre operators wishing to operate an internal fibre-based telecommunications network must obtain a special telecommunications licence.

STRATEGIC OPPORTUNITIES

05. FOREIGN INVESTMENT RESTRICTIONS

Structure and capital requirements

Foreign companies typically conduct business in Indonesia by setting up a local foreign limited liability company (or **PT PMA**). Setting up one of these companies:

- requires paid-up capital of at least IDR10 billion (roughly US\$700,000), and
- typically takes a minimum of a month.

Land

Corporate entities (including PT PMAs) cannot acquire rights of ownership for land – only Indonesian individuals may own land outright.

HOWEVER, PT PMAS CAN ACQUIRE THE ‘RIGHT TO BUILD’ (*HAK GUNA BANGUNAN* OR HGB) ON LAND, BEING RIGHTS TO CONSTRUCT AND OWN BUILDINGS ON LAND FOR UP TO 30 YEARS, WITH A POSSIBLE 20-YEAR EXTENSION AND SUBSEQUENT RENEWAL FOR A 30-YEAR TERM.

Data centres

Otherwise, there are no specific foreign investment restrictions related to owning or operating data centre businesses in Indonesia. Foreign investors can:

- set up companies including PT PMAs
- construct and own buildings on land (if they purchase the rights to build), and
- construct and own buildings for up to 80 years (subject to renewals after 30 years).

06. TAX INCENTIVES

Special economic zones

Indonesia has established SEZs (*Kawasan Ekonomi Khusus*) to attract investment in certain areas such as the digital economy, offering simplified regulatory processes, infrastructure support and tax incentives. Data centres are likely to qualify to access these benefits.

SEZ BUSINESSES BENEFITS - EXAMPLES	
FISCAL INCENTIVES	NON-FISCAL INCENTIVES
<ul style="list-style-type: none">• Relaxed VAT• Luxury Goods VAT• Import tax• Excises• Regional tax	<ul style="list-style-type: none">• ‘One-stop shop’ for obtaining licenses• Streamlined import restrictions licensing processes• Relaxed building licenses• Longer working permits

Not all SEZs qualify as industrial estates. *Law No. 39 of 2009 on Special Economic Zones* provides that SEZs may be designated for various purposes, including production and processing, logistics and distribution, technological development, tourism, education, health, energy and/or other economic sectors.

At present, the following SEZs are specifically designated for the digital technology industry and are categorised as industrial estates:

- **Nongsa SEZ** – Nongsa SEZ or Nongsa Digital Park (**NDP**) is an integrated area for digital businesses located in Nongsa, Batam, and
- **Singhasari SEZ** – Singhasari SEZ, located in Malang Regency, Indonesia, is located near Juanda International Airport in Surabaya and Tanjung Perak Port, and is connected by the Pandaan-Malang toll road.

Industry-specific incentives

Investments in the digital economy, including data processing and hosting activities, can qualify for a tax allowance under the *Minister of Finance Regulation No. 130/PMK.010/2020*. This requires a minimum investment of 100IDR billion (approximately US\$6 million). More information is available at the [government’s ‘Investment in SEZ’ website](#).



COMPLIANCE AND RISK MANAGEMENT

07. DATA PROTECTION AND CYBER SECURITY

Universal data protection or privacy laws

Indonesia's *Law No. 27 of 2022 concerning Personal Data Protection (PDP Law)* is generally applicable in Indonesia. The exposure of a data centre operator to the PDP Law depends on the extent of the operator's ability to access or manipulate customer data.

For **pure colocation arrangements**, where the customer uses colocation space and services provided by the operator, and performs data processing itself, the **practical exposure to the PDP Law is minimal**. Cloud service providers and hosting service providers, on the other hand, are more likely to be considered data processors, captured by the PDP Law.

The PDP Law requires data controllers and data processors to use **technical and operational measures** to ensure security of data they hold.

FURTHER GUIDANCE IS EXPECTED TO COME UNDER GOVERNMENT REGULATIONS AND STANDARDS TO BE PUBLISHED BY A NEW DATA PROTECTION AUTHORITY, THE PDP INSTITUTION. THIS HAS NOT YET BEEN ESTABLISHED AT THE TIME OF PUBLICATION, DESPITE BEING MANDATED BY THE PDP LAW.

International standards

The Indonesian government has adopted various ISO/IEC international standards on security as national standards for Indonesia (ISO 27001, ISO 27002, ISO 18033-1 through 18033-6), but compliance with them is not mandatory.

Industry practice is for data centres (and their customers) to comply with international standard ISO 27001:2002 in relation to security.

Operational resilience obligations

General requirements for operational resilience under *Government Regulation No. 71 of 2019* apply to electronic system operators, including data centres. These obligations involve maintaining audit trails, securing system components and ensuring system functionality.

08. CRITICAL INFRASTRUCTURE AND SECURITY

In Indonesia, 'National Vital Objects' (**Obvitnas**) are considered critical infrastructure that may be eligible to receive police and military protection from the government in the event of an internal or external threat.

Data centres will only be Obvitnas if specifically designated by a ministerial decree or a decree of a non-ministerial government institution.



09. DATA LOCALISATION

There are various targeted data localisation requirements in Indonesia.

ORGANISATIONS	ARE REQUIRED TO	UNDER REGULATION
DATA CENTRES APPOINTED TO PROVIDE SERVICES TO GOVERNMENT <i>public electronic system operators</i>	Manage, process and store data within Indonesia. Certain data may be stored offshore, but public electronic systems operators must provide the Indonesian government with access to that data.	<i>Government Regulation No. 71 of 2019</i>
BANKS	Locate data centres and disaster recovery centres in Indonesia, unless the Financial Services Authority (<i>Otoritas Jasa Keuangan</i> or OJK) grants approval for them to be located offshore.	<i>OJK Regulation No. 11/POJK.03/2022 on Information Technology Implementation by Commercial Bank</i>
NON-BANK FINANCIAL SERVICES INSTITUTIONS This includes insurance companies, pension funds, financing institutions, pawnbrokers, guarantee institutions, peer-to-peer lending providers, Indonesia's export financing institutions, mortgage-backed security and social security agencies.	Locate data centres and disaster recovery centres in Indonesia unless they obtain approval from the OJK to use offshore data centres or disaster recovery sites.	<i>OJK Regulation No. 4/POJK.05/2021 on the Implementation of Risk Management in Using Information Technology by Non-Bank Financial Services Institutions, as partially and lastly revoked by OJK Regulation No. 40 of 2024 on Information Technology Based Joint Funding Services</i>
PAYMENT SERVICE PROVIDERS	Locate electronic systems used for transaction processing at the initiation, authorisation, clearing, and final settlement stages in a data centre and disaster recovery centre in Indonesia.	<i>Bank Indonesia Regulation No. 23/6/PBI/2021 on Payment Systems Providers</i>
FINTECH INNOVATION PROVIDERS (<i>Penyelenggara Inovasi Teknologi Sektor Keuangan</i> or ITSKs)	Locate data centres and disaster recovery facilities in Indonesia.	<i>OJK Regulation No. 3/POJK.02/2024 on the Implementation of Technological Innovation in the Financial Sector</i>
HEALTHCARE FACILITIES	Only store data in Indonesia.	<i>Ministry of Health Regulation No 24 of 2022 on Medical Records</i>

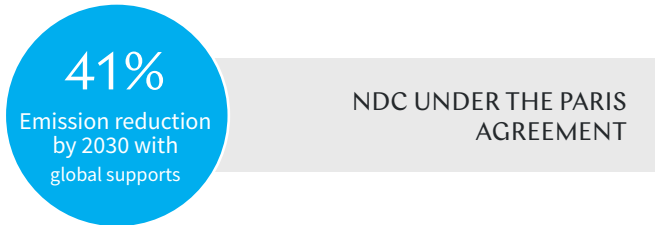


10. ENVIRONMENTAL, SOCIAL AND GOVERNANCE

International ESG commitments

Indonesia is a signatory to the Paris Agreement, which has been ratified in domestic law in Law No. 16 of 2016. Under Article 3 of the Paris Agreement, Indonesia has committed to various measures in its NDC, although these have not been enacted in domestic law. Specific commitments in the NDC include:

- reducing its carbon emissions by transitioning to renewable energy sources, and
- developing Indonesia’s technology sector.



Environmental management and monitoring

Data centre developers must implement a Detailed Environmental Management Plan-Environmental Monitoring Plan (*Rencana Kelola Lingkungan-Rencana Pemantauan Lingkungan Rinci* or **RKL-RPL**) as a prerequisite for constructing a data centre or obtaining the business licences required to operate a data centre.

ESG reporting

Currently, there are no specific ESG-related reporting requirements for data centres in Indonesia.

Energy efficiency and conservation

High energy consumption businesses like data centres are subject to the energy conservation requirements of GR33/2023 (see [Section 1](#), Power above).



11. SECTOR-SPECIFIC REGULATIONS APPLICABLE TO DATA CENTRES

Government bodies

Data centre operators providing services to government bodies may be required to comply with regulations requiring government bodies to prioritise domestic suppliers in procuring products and services.

Financial services providers or financial institutions

Financial institutions in Indonesia must comply with regulations that require oversight of third-party IT service providers. Data centres providing services to financial institutions are subject to compliance checks, including audits and disaster recovery plans, as stipulated by OJK regulations.

Digital asset providers, digital certification bodies and digital ID providers

Sector-specific regulations for digital asset providers, digital certification bodies, and digital ID providers do not directly impose obligations on data centres. However, these customers may impose specific compliance requirements on data centre operators to meet their regulatory obligations, such as data security and operational standards.

INDONESIA IS A DYNAMIC ECONOMY WITH INCREDIBLE POTENTIAL... TENCENT [IS COMMITTED] TO PARTNERING INDONESIA IN ITS DIGITAL TRANSFORMATION JOURNEY TO TAP THE IMMENSE POTENTIAL OF THE AI REVOLUTION TO EMPOWER LOCAL ENTERPRISES WITH RELIABLE CLOUD AND AI-POWERED SOLUTIONS.

POSHU YEUNG,
[TENCENT CLOUD INTERNATIONAL SENIOR VICE PRESIDENT](#) ON SIGNING AGREEMENTS WITH GOTO GROUP AND ALIBABA CLOUD TO WORK TOGETHER TO BOOST INFRASTRUCTURE IN INDONESIA.



JAPAN

CHAPTER 6

SNAPSHOT



Japan's data centre market was the third largest worldwide in 2024 by revenue, sitting behind only the US and China. The same year, Tokyo was the most popular market among surveyed data centre investors within the APAC region.

Much of the market's growth is due to Japan's political stability, strong local talent and wide acceptance of AI. This is complemented by a clear regulatory framework with limited restrictions on critical infrastructure and foreign investment.

While subsidies are generally limited, they exist for the development of data centres outside of Tokyo and Osaka, and for

government infrastructure, as highlighted by the JPY600 million (~US\$4 million) subsidy to data centre operator SAKURA Internet.

Power supply presents a challenge, particularly in Tokyo. Combined with rising construction and land costs and a tight labour market, this can significantly delay development.

A further complication is the propensity for natural disasters in Japan such as earthquakes and tsunamis, which can cause significant power outages. Despite these difficulties, outside of the data centre dense areas of Tokyo and Osaka, Japan is an attractive destination for development.

OPPORTUNITIES

- ✓ Clear regulatory framework and stable economy
- ✓ Limited restrictions on foreign investment and critical infrastructure
- ✓ No data localisation requirements

CHALLENGES

- ✗ Power supply carries significant delays and costs
- ✗ Rising costs of land and construction
- ✗ Limited incentives

SPOTLIGHT ON KEY DRIVERS

REGULATORY CLARITY AND CONFIDENCE

Japan's commitment to regulatory transparency and its stable economic and legal environment make it an attractive destination for data centre developers and operators.

Japan offers clear standards for data protection and cyber security, along with a supportive approach to innovation.

The government has been openly hesitant of hindering innovation and creating excessive burden in connection with AI. They have recently enacted a law specifically focused on government-led promotion measures for AI, the *Act on Promotion of Research, Development and Utilisation of Artificial Intelligence-Related Technology*.

This is bolstered by industry-led efforts. Notably, the Japan Data Centre Council's voluntary Data Centre Facility Standard is focused on ensuring and improving the quality and reliability of the design, construction and operation of data centres.

OPEN TO FOREIGN INVESTMENT

Japan's commitment to foreign investment openness is a significant drawcard for international capital in the data centre sector.

Japan imposes no restriction on foreign ownership of land, allowing offshore investors to acquire property. In cases where foreign-ownership notification to the relevant minister is required, approval is rarely withheld.

Nonetheless, foreign players should understand that Japan is a very localised market. Knowledge of, and respect for, cultural norms and business practices is critical for success.

CHAMPIONING DATA FLOW WITHOUT BORDERS

The Japanese Government has adopted a policy position of promoting the free flow of data via the concept of Data Free Flow with Trust (DFFT).

It does not provide data localisation regulations or require government access to data. This may increase the attractiveness of politically independent Japanese data centres to overseas players. However, there is a limited likelihood that users will see Tokyo as a potential regional hub given the high costs of power.

'Investment in data centres is rapidly increasing due to rising AI demand, with major tech firms and foreign companies making significant commitments. This growth is supported by government AI policies and flexible copyright laws. However, the rise in data centres has raised electricity use concerns, prompting the government to consider energy-saving regulations and promote decentralisation, as 80% are concentrated in the limited areas of Tokyo and Osaka, making them vulnerable to disasters.'

Yoshiki Tsurumaki
Partner
King & Wood Mallesons



OPERATIONAL

01. POWER

Getting power to a site

Japan has a competitive electricity market with multiple private power companies and retail electricity providers. Despite this, there are availability and cost hurdles.

Securing **reliable electricity supply** can face significant delays, particularly in Tokyo and other major cities. Grid capacity limitations, aging infrastructure, lengthy approval and permitting processes and strict zoning and environmental laws all contribute to a prolonged development and construction process, particularly when new infrastructure is required.

IN TOKYO, WHERE TOKYO ELECTRIC POWER COMPANY'S (TEPCO) GRID CANNOT SCALE AT THE RATE OF DEMAND, THIS PROCESS CAN CURRENTLY TAKE OVER 10 YEARS IN SOME CASES.

The **application process** varies depending on the provider, but the contractual terms are usually standard form and not negotiable.

The **significant price** of power in Japan means that domestic applications are likely to take priority in Japanese data centres, effecting capacity and making it challenging for customers to use Japanese data centres as a regional hub from a cost perspective.

Power purchase agreements

In Japan, data centre developers can enter 'normal' supply contracts with retailers or corporate PPAs.

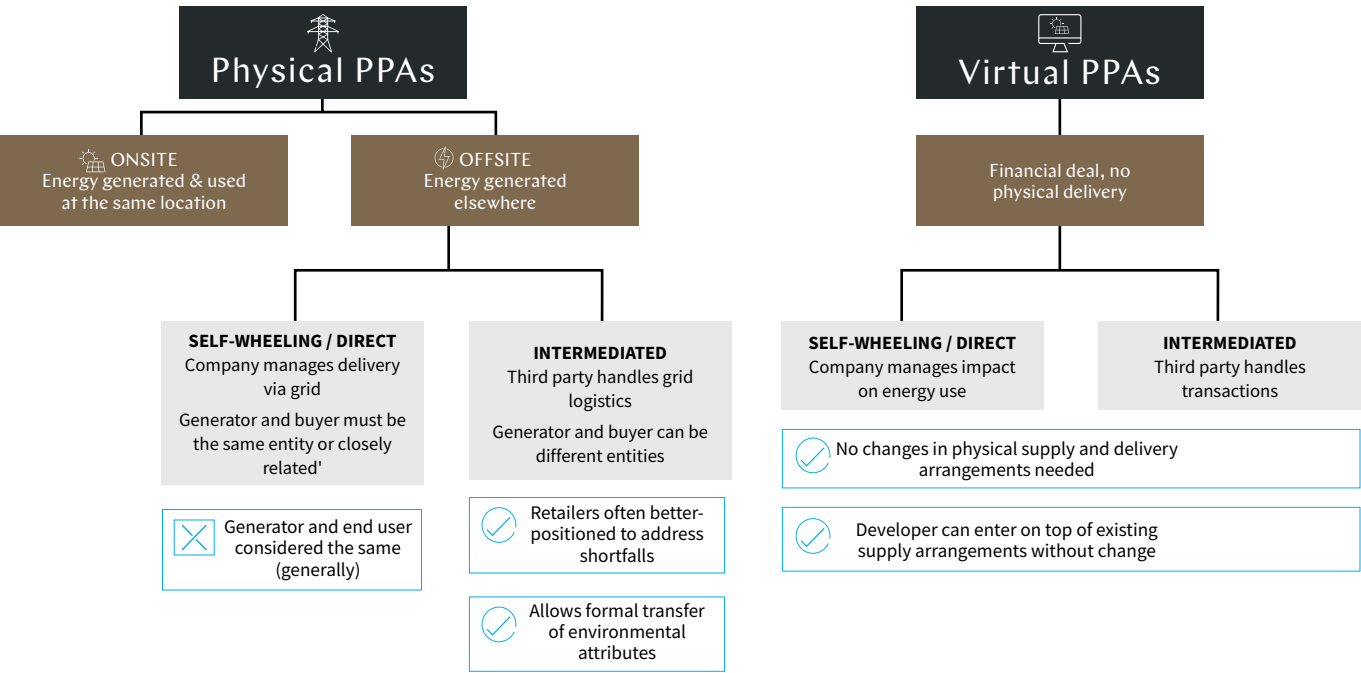
Corporate PPAs can be corporate physical PPAs, or corporate virtual PPAs. End users, including data centre developers and their customers, are expected to increasingly use all forms of corporate PPAs as they take steps to address net zero objectives, electricity supply and pricing challenges.

Corporate virtual PPAs represent the newest evolution in Japan's renewable electricity procurement landscape and can retail intermediated or direct, like corporate physical PPAs. However, unlike corporate physical PPAs, they do not require changes in the physical supply and delivery arrangements of the generator or the purchaser, meaning that a data centre developer can enter into a corporate virtual PPA on top of its existing supply arrangements often without changing them.

Direct corporate virtual PPAs have gained popularity since 2022, when legislative changes allowed the direct transfer of environmental attributes from the generator to the buyer.

The Ministry of Economy, Trade and Industry (METI) also issued an interpretation confirming that in its view corporate virtual PPAs are not in principle OTC derivative transactions regulated under the *Commodity Derivatives Transaction Act* if they provide for the transfer of a 'substantive' environmental value on a verifiable basis.

NAVIGATING CORPORATE PPA OPTIONS



Promoting a more decentralised and sustainable future

In 2023, 80% of data centres in Japan were concentrated in Tokyo and Osaka, creating an uneven distribution of power loads and causing stress on the grid. To decentralise this concentration, and to tap into clean energy supply located in other regions, the METI is actively promoting the development of data centres outside of Tokyo by offering substantial subsidies.

Areas of focus for subsidies include Hokkaido and Kyushu, which have rich renewable energy resources, such as hydropower, solar, geothermal and offshore wind (see section 6, tax and other incentives, below for details of the subsidies available)

PUE and energy consumption reporting

The *Energy Use Act*:

- sets a target PUE of ≤ 1.4 for data centres by 2030
- requires data centres (and other designated businesses) whose annual energy consumption (converted to crude oil equivalent) $\geq 1,500$ kilolitres to submit a Notification of Energy Usage. Upon submission, a business may be designated as a Specified Business. Once designated, businesses must:
 - appoint an Energy Management and Supervision Officer and an Energy Management Planning Promoter, and
 - submit both a medium-to-long-term plan and engage in regular reporting (although regular reporting is not required if the total server room area is under 300m² at a given place of business), and
- encourages long-term reductions by incentivising top-performing companies through a **class-based evaluation system**, where operators achieving an 'S Class' rating—based on energy intensity improvements or meeting benchmark standards—for 2 or more fiscal years are rewarded. This may include being exempt from submitting medium-to-long-term plans for up to 5 years, provided the 'S Class' rating is maintained.

Importantly, a further legal amendment is being considered, which would make compliance with minimum energy performance standards mandatory for new data centres from FY2029 onward.

02. WATER

Water supply

Water supply is a matter for the local water authorities. The process and requirements vary depending on where the site is located, but generally speaking:

- developers must use the specific local supplier
- connection may be subject to limitations depending on local infrastructure, capacity, and regulations, and
- water suppliers must make their relevant terms of service, including rates, open to the public and are required to provide water to consumers within their service area when an application for supply is made under the *Water Supply Act 1957*.

Water reserves recommended

While there are no specific guidelines on water usage in data centres, the voluntary Data Centre Facility Standards provide a list of recommended items for a data centre which include a 'make-up water reserve' for air conditioning.



ON THE GROUND

LETTING GO OF HEAT – BY LETTING IT SNOW

The White Data Centre (WDC) in Bibai City, Hokkaido uses snow to cool its facilities of approximately 20 racks of servers. The WDC uses snow removed from the street by the local government to create a large, insulated mound outside the data centre. The snow is used as a cold thermal source to indirectly cool a water-based circulation system.

Warm water heated by the servers is routed through a series of cooling stages, including agricultural heat recovery, air cooling towers, and ultimately through a heat exchange system located beneath the snow mound. There, the latent heat of fusion from the snow is used to lower the temperature of the circulation water without direct contact.

This cools the data centre's servers using half the energy required by conventional techniques, with no CO₂ emissions, greatly reducing the WDC's PUE to 1.04 in summer, 1.05 in winter and 1.15 in spring and autumn.



03. LAND



WHERE CAN DATA CENTRES BE BUILT?

Japan classifies land into 13 use zones, which are broadly grouped into residential, commercial and industrial zones.

Data centres:

- **are permitted** in quasi-industrial, industrial, and exclusive industrial zones – these are the most common and practical zones for data centre development
- **may be permitted** in commercial or mixed-use zones, depending on the specific use classification, size, and local government interpretation - additional permissions may be required in these zones, and the process can be complex and uncertain, and
- **generally are not permitted** in residential zones.

More generally, there are restrictions under more than 60 laws and ordinances, including the:

- *City Planning Act 1968 (City Planning Act)*
- *the Building Standards Act 1950 (Building Standards Act)*, and
- *Landscape Act*.

Therefore, from a practical perspective, there is limited land available that is of an appropriate size and in a desirable location for a data centre. This has posed challenges for prospective investors and developers sourcing land.



WHAT APPROVALS AND PERMITS ARE REQUIRED AND HOW LONG DO THEY TAKE?

- If a data centre **exceeds a certain size**, development approval is required and this includes a process of community consultation. This approval process may take 6 to 12 months under the City Planning Act.
- Approval from the Minister of Land, Infrastructure, Transport and Tourism, or a designated approval body, may also be necessary where for example, **certain types of building materials or structural methods are used**, extending the development timeline by several months. This is under the Building Standards Act, which also requires a public hearing.
- When constructing a data centre on **privately owned forest land subject to a Regional Forest Improvement Plan**, developers must obtain permission from the relevant Prefectural Governor before carrying out activities that alter the land, such as excavation or reclamation.
- The Governor must grant permission unless the proposed activity poses risks related to disaster prevention, flood control, water source recharge, or environmental conservation. If these risks exist, permission may not be granted, to protect the surrounding area. This is under the *Forest and Forestry Basic Act 1964*.

04. TELECOMMUNICATIONS

Is a telecommunications licence required?

Data centre operators are required to:

- **register** with the Ministry of Internal Affairs and Communications (**MIC**) as a telecommunications business if they conduct a telecommunications business (by providing telecommunications services for its customers)
- **notify** the MIC if they provide telecommunications services, but their transmission facilities are limited to a single municipality (for terminal facilities) or a single prefecture (for relay facilities), or
- **protect the security of communications** only (that is, no registration or notification is required) if the service only uses telecommunications facilities without installing line facilities and does not mediate third-party communications.

Data centres that provide **hosting or colocation services only** **are unlikely** to conduct a telecommunications business and therefore are not required to register, notify or protect the security of communications.

Applicability of telecommunications laws to data centres

The *Telecommunications Business Act (Telecommunications Act)* applies to data centre operators or developers if they provide services requiring them to be registered with the MIC. If registration is required, data centre operators must, amongst other things:

- comply with technical standards
- establish administrative regulations for those technical standards and notify the MIC of those regulations prior to commencing business, and
- appoint a chief telecommunications engineer.

STRATEGIC OPPORTUNITIES

05. FOREIGN INVESTMENT RESTRICTIONS

Land

There are no foreign investment restrictions on land ownership in Japan.

Data centres

Foreign investors must obtain government approval before acquiring an interest in certain ‘designated business sectors’ under the *Foreign Exchange and Foreign Trade Act 1949 (FEFT Act)*.

Designated business sectors for data centres includes the provision of:

- information technology services
- telecommunications services
- handling of critical infrastructure (for example, for defence, energy, finance or government), or
- information processing services.

What does the process look like?

This process is more akin to a pre-screening process than an approval, but the government may impose restrictions or conditions on the relevant investment.

Are there any exemptions?

There are some, including if the investor does not take a position as an officer of the company or if they are restricted from accessing non-public technology related information of the company.

However, a recent change means that the government now classifies investors who may cooperate with foreign governments in gathering information as ‘Specified Foreign Investors’. These Specified Foreign Investors are unable to obtain an exemption, meaning that all their investments will require preliminary screening.

The foreign investment restrictions that apply to data centres also apply to cloud service providers.

06. TAX AND OTHER INCENTIVES

Decentralisation incentives

As part of the government’s decentralisation efforts to push and strengthen regional digital infrastructure, subsidies are available for large-scale data centre projects located on land parcels of ≥10 hectares.

- Under the **Data Centre Infrastructure Development Project**, eligible projects may receive support covering up to ¥15.54 billion (~US\$108 million) to off-set infrastructure-related costs.
- Where both the **Data Centre Infrastructure Development Project** and **Facility Development Project** are applied in combination, the total available subsidy may increase to up to ¥30 billion (~US\$208 million), covering both infrastructure and facility construction.

SOFTBANK RECEIVED A ¥30 BILLION SUBSIDY UNDER THIS PROGRAM FOR THE CONSTRUCTION OF A 50MW (WITH PLANS TO SCALE TO 300MW) DATA CENTRE IN TOMAKOMAI CITY, HOKKAIDO.

Energy efficiency and renewable incentives:

Ministry of Environment (**MOEJ**) offers subsidies aimed at enhancing the environmental performance of data centres. These initiatives focus on promoting energy efficiency and the adoption of renewable energy sources and are available to businesses that install renewable energy and energy storage systems or low CO₂ equipment, such as energy efficient cooling systems, in the construction or renovation of data centres.

Government infrastructure systems:

METI offers subsidies through the ‘Government Cloud’ and ‘Cloud Program,’ for entities providing government and local government infrastructure systems.

IN 2023, SAKURA INTERNET INC, WAS THE FIRST DOMESTIC PROVIDER OF THE ‘GOVERNMENT CLOUD’ AND RECEIVED A ¥600 MILLION (~US\$4 MILLION) SUBSIDY.



COMPLIANCE AND RISK MANAGEMENT

07. DATA PROTECTION AND CYBER SECURITY

Data protection or privacy laws

Businesses handling personal information must securely manage the personal information that they hold, under the *Act on the Protection of Personal Information* (**Personal Information Act**).

Sending information offshore: This includes requiring businesses that transfer personal information off-shore to inform the individual about how their personal information is protected by the laws in the off-shore jurisdiction and to obtain the individual's consent.

Managing important systems: The Personal Information Guidelines also require the appropriate management of important information systems such as servers and main computers that handle personal information.

Practically, if a data centre operator is providing colocation services only, it is unlikely to trigger any material regulatory requirements, and these requirements are more likely to apply to *customers* of data centre operators rather than the operators themselves. Cloud service providers or managed hosting providers are more likely to need to comply, if they collect or handle personal data.

Breach notification obligations

Unauthorised access to personal information on data servers must be reported to the Personal Information Protection Commission.

08. CRITICAL INFRASTRUCTURE AND SECURITY

Critical infrastructure laws

If the data centre is a major telecommunications carrier under the Telecommunications Act, it is considered by the National Centre of Incident Readiness and Strategy for Cybersecurity (**NISC**) to be critical infrastructure.

The NISC aims to promote and coordinate cyber security policies, including the Cybersecurity Policy for Critical Infrastructure Protection. The Fundamental Plan for National Resilience 2023 also covers physical and cyber threats to infrastructure including telecommunications.

However, there are currently no specific laws in force or bills pending, as of the date of this publication, that regulate data centres in relation to critical infrastructure on a general basis.

The *Cyber Incident Response Enhancement Act* was enacted by Diet in May 2025, but is not yet in force. The Act aims to establish clear protocols for incident reporting and data analysis and strengthen Japan's resilience against cyber threats.

Importantly, it requires designated essential infrastructure service providers to report both specific cyber security incidents and information such as product names of Specified Critical Computer Systems that they use. Once in force, it is likely that this Act will have a significant impact on data centres.

09. DATA LOCALISATION

Allowing data to flow without restrictions

There are no regulations concerning data localisation or residency in Japan. Instead, the Japanese government supports the concept of DFFT.

DFFT is a concept which aims to promote cross-border data flows whilst ensuring trust in privacy, data protection and security measures. It was first introduced by former Japanese Prime Minister Shinzō Abe during his speech at the World Economic Forum in Davos in 2019. DFFT has since been embraced by international bodies like the G7, G20 and OECD.

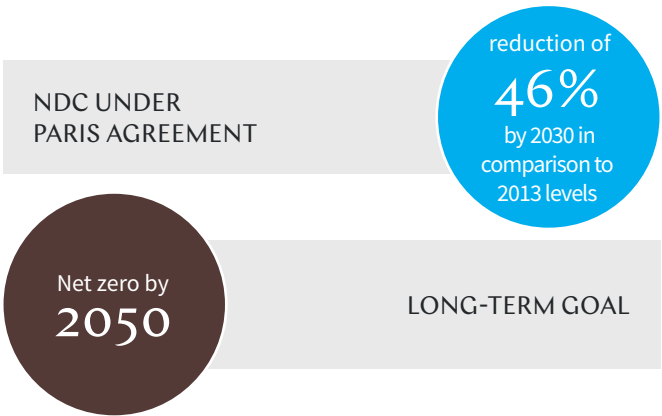
Targeted data localisation requirements

Providing regulated technical information, such as information likely to be used in development of weapons of mass destruction, to non-residents requires prior permission from METI under the FEFT Act. Breaches can lead to administrative penalties and criminal sanctions.

10. ENVIRONMENTAL, SOCIAL AND GOVERNANCE

International ESG commitments

Japan is a signatory to the Paris Agreement, implementing these commitments into domestic law in the Act on Promotion of Global Warming Countermeasures 1998.



Voluntary technical standards or accreditations

The Data Centre Facility Standard, formulated by the Japan Data Centre Council, is a widely used voluntary guideline for ensuring and improving quality and reliability of the design, construction and operation of data centres. The Standard focuses on:

- ensuring that facilities are disaster resilient
- access control systems protect the building and server room
- backup systems ensure the facility continues to operate during power outages or maintenance, and
- the data centre maintains a high level of service reliability for end users.



11. SECTOR-SPECIFIC REGULATIONS APPLICABLE TO DATA CENTRES

Government bodies

Government-related agencies are generally required to procure cloud services from providers listed in the Information System Security Management and Assessment Program (**ISMAP**).

To be registered on the ISMAP Cloud Service List, service providers must pass both:

- an **external audit** by meeting ISMAP's management standards, and
- a **compliance test** by the ISMAP Steering Committee.

Financial services providers or financial institutions

The Guidelines on Cybersecurity in the Financial Sector (**Guidelines**), established by the Financial Services Agency apply to financial institutions, banks and securities firms and are intended to promote the development and strengthening of cyber security measures at financial institutions. Parts of the Guidelines apply indirectly to data centres.

Digital asset service providers (including cryptocurrency exchanges)

The *Payment Services Act 2009* (**Payment Services Act**) applies to issuers of prepaid payment instruments and cryptocurrency exchange service providers, requiring them to implement security management measures to prevent leakage, loss or damage to information pertaining to the business of issuing prepaid payment instrument and relevant information.

The Payment Services Act includes specific considerations that must be taken into account when selecting external contractors, including data centres.

Healthcare

The Guidelines for the Secure Management of Medical Information Systems require medical institutions and related businesses, when storing medical information externally, to:

- verify the security practices of their system providers (including data centres), and
- select providers that comply with the Guidelines for the Safety Management of Providers of Information Systems and Services Handling Medical Information, established by METI.



MALAYSIA

CHAPTER 7

SNAPSHOT | A REGIONAL DATA CENTRE HUB EMERGES



Malaysia is rapidly emerging as one of the most dynamic data centre markets in Southeast Asia. In the first 10 months of 2024 alone, the country recorded an astounding US\$32 billion in digital sector investments, tripling the total investments for 2023. This surge is largely driven by hyperscalers such as Microsoft, Amazon Web Services, Google and Oracle, who have collectively invested US\$23.3 billion to date.

With its strategic proximity to Singapore, particularly Johor, and favourable policies and economic incentives, Malaysia has become a regional data centre hub. Yet with such rapid growth comes sustainability pressures. Malaysian federal and state governments are seeking to tackle these head-on.

OPPORTUNITIES

- ✓ 'Singapore Plus' demand
- ✓ Strong political support in Johor
- ✓ GPU-as-a-service models

CHALLENGES

- ✗ AI export controls
- ✗ Different state rules
- ✗ Sustainability challenges

SPOTLIGHT ON KEY DRIVERS

LOCATION, LOCATION, LOCATION

Investment into Johor is exploding as a proximate, cost-effective and attractive alternative to Singapore.

Singapore's moratorium on new data centre developments from 2019 to 2022, imposed due to concerns over land availability and high energy consumption, led to spillover demand from global hyperscalers and data centre operators into nearby Johor. Despite Singapore lifting the moratorium by adopting a selective and sustainability-focused approval process for new developments, the trend continues.

It is not all about Johor. Klang Valley remains the largest data centre market in Malaysia.

GOVERNMENT INCENTIVES

Strong government support and strategic initiatives have helped to attract investment and foster growth.

Developers and operators can take advantage of various deep incentives, including:

- Malaysia Digital Status (**MDS**) offering tax and other incentives
- Digital Ecosystem Acceleration Scheme (**DESAC**) providing tax allowances and reduced tax rates
- The recently formed Johor-Singapore SEZ introducing further benefits for developers including special corporate tax rates, cross-border process improvements and other customised incentives.

SUSTAINABILITY CHALLENGES

Malaysia remains heavily dependent on fossil fuels with limited renewable capacity.

Power costs are relatively low, but explosive growth in the industry poses energy supply and grid stability issues.

Energy efficiency and sustainable growth are the key focus of a range of reforms introduced by the Malaysian government, particularly in energy-intensive industries like data centres.

Water usage limits for data centre operations are part of proposed planning reforms by Malaysia's National Water Services Commission (**SPAN**).

'Malaysia is rapidly emerging as Southeast Asia's next data centre powerhouse, driven by a surge in AI and cloud computing investments. Johor Bahru, in particular, is transforming into the region's fastest-growing data centre market, attracting tech giants like Microsoft, Google and Nvidia'

Tan Wei Xian
Partner
Skrine



OPERATIONAL

01. POWER

Getting power to a site

This process depends on location. The main electricity provider is Tenaga Nasional Berhad (**TNB**), covering Peninsular Malaysia and East Malaysia via a subsidiary. Sarawak Energy Berhad is the provider for Sarawak. They each have a monopoly on transmission, distribution and retail in their respective territories.

In addition, Sarawak Energy Berhad has a monopoly on generation in its territory.

Power purchase agreements

By way of exception to the territorial monopolies above, generators and users can enter:

- corporate onsite physical PPAs for electricity generated **on the site** of the user, or
- in Peninsular Malaysia, corporate offsite physical PPAs for electricity generated **outside of the site** of the user and transported through the grid.

The Malaysian government has initiatives to boost green energy use, offering pathways for generators and users to enter corporate offsite and corporate virtual PPAs.

- Corporate offsite physical PPAs can be implemented under the **Corporate Green Power Programme** (for generation facilities of between 5MW and 30MW, closed for applications in 2023) and the **Corporate Renewable Energy Supply Scheme** (for generation facilities above 30MW, opened for applications in 2024) following a successful application.
- Under either scheme the generator and the user can enter a corporate virtual PPA known as a ‘Corporate Green Power Agreement’ (under CGPP) or a ‘Bilateral Energy Supply Contract’ (under CRESS), the terms of which must address the requirements of the relevant scheme/programme. In either case the user must still have a supply contract with TNB. There are no similar schemes outside of Peninsular Malaysia.

Going ‘green’

The Guidelines for Sustainable Development of Data Centres (**SDDC Guidelines**) set best practices and standards for developing and operating sustainable data centres, encouraging the integration of renewables and the use of efficiency measures based on the category and size of the data centre. Data centres must meet specific thresholds for PUE, Carbon Usage Effectiveness (**CUE**) and Water Usage Effectiveness (**WUE**) values which vary by category.

Issued by the Ministry of Investment, Trade and Industry, SDDC Guidelines compliance is a factor (until 31 December 2027) in qualifying for tax incentives under the DESAC (see [Section 6](#) Tax and other incentives below).

All **new data centres**, regardless of category, must be located in areas with a water stress index below 0.8 within Peninsular Malaysia.

Hyperscale data centres have targets of PUE of 1.4 or lower, WUE of 2.2m3/MWh or lower, and power capacity above 21.25MW.

Enterprise private (captive) data centres in purpose-built or converted building have targets of PUE of 1.7 or lower, WUE of 2m3/MWh or lower, and power capacity of between 0.85MW and 4.25MW.

The Guidelines Specification for Green Data Centres (**GDC Specification**) is a voluntary code issued by the Malaysian Communications and Multimedia Commission (**MCMC**) and provides benchmarking standards for green data centres. This covers PUE, air temperature and humidity range, as well as governance, reporting, training and policy compliance requirements. The GDC Specification recommends that developers and operators implement an energy management system in accordance with ISO 50001.

Certification by a **Malaysian Green Building Index Certifier** is also common to evaluate the energy efficiency, water conservation and waste reduction based on a detailed set of criteria.

PENINSULAR MALAYSIA	EAST MALAYSIA (SABAH & LUBUAN)	SARAWAK
Electricity provider		
TNB	Sabah Electricity Sdn Bhd (TNB subsidiary)	Sarawak Energy Berhad
Process for bulk power supply		
Electricity supply agreement (TNB’s standard form) usually required 36-48 month process May require developer to construct a substation		
Fast-track implementation process TNB Green Lane Pathway		
12 months Reduces electricity procurement process time		

‘MALAYSIA IS BECOMING A REGIONAL HUB FOR MANY BUSINESSES, AND THIS IS DRIVING MORE ORGANISATIONS TO INVEST IN CLOUD SYSTEMS, WHICH ARE, IN TURN, DRIVING THE NEED FOR MORE LOCAL DATA CENTRES.’

02. WATER

Water supply

Procurement of water supply is a matter for each state of Malaysia. The process, requirements and timeline for procuring water supply for a data centre project varies between states.

Water guidelines

The SDDC Guidelines contain water usage effectiveness standards and encourage the reuse of reclaimed water.

The Planning Guideline for Data Centres (**Planning Guideline**) requires developers to seek advice and comments from the SPAN when obtain planning approval.

The SPAN has also proposed (but has not implemented) regulatory measures to **limit water usage in data centre operations** to support a sustainable national water supply. As part of these measures, SPAN has recommended that local authorities assess the adequacy of water resources at proposed data centre sites during the planning approval process, including factors such as the availability of water sources in the area and the data centre’s ability to secure alternative water resources.



03. LAND

WHERE CAN DEVELOPERS BUILD DATA CENTRES?

The Planning Guideline provides that data centre development is permitted on land subject to the categories ‘building’ or ‘industrial’ use. If the title to the land is endorsed to allow other use or development, a special permit may be required from the relevant state authority or the title conditions may need to be varied under the Malaysian National Land Code.

WHAT IF RE-ZONING IS NEEDED?

The Planning Guideline provides that data centre development is allowed in industrial land use zones (light and medium) and commercial land use zones. Re-zoning is possible under the *Town and Country Planning Act 1976*. The relevant local planning authority may hold hearings and hear objections to proposed re-zoning. The time required to re-zone varies by local authority and an objection to any proposed re-zoning can cause delays.



HOW LONG DOES IT TAKE TO GET PERMITS OR VARY CONDITIONS?

The time required to obtain special permits or variations to title conditions varies by state. In Johor, a data centre development requires approval of Johor’s Data Centre Development Coordination Committee which may take into consideration factors such as sustainability plans (including power, water and carbon usage effectiveness) and job creation metrics.

WHAT ARE THE LOCATION CONSIDERATIONS?

The Planning Guideline requires that data centre sites are close to infrastructure and utilities, including electricity supply, and to include setback and buffer zones to mitigate environmental impacts. Issued by the Ministry of Housing and Local Government, through the Department of Town and Country Planning, the Planning Guideline is considered by state and local authorities when granting approvals for data centre developments. They also require developers to obtain TNB approval for a site.

04. TELECOMMUNICATIONS

Applicability of telecommunications laws to data centres

The *Communications and Multimedia Act 1998* does not generally apply to data centre operators or developers unless they provide services requiring a telecommunications licence (see below).

Is a telecommunications licence required?

Only if the data centre operator or developer:

- provides an internet access services or hosts cloud services on behalf of a foreign cloud provider where an Application Service Provider (**ASP**) licence is required
- provides bandwidth services where a Network Service Provider (**NSP**) licence is required, or
- owns, operates, maintains, installs or provides network facilities such as fibre cables where a Network Facilities Provider (**NFP**) licence is required.



STRATEGIC OPPORTUNITIES

05. FOREIGN INVESTMENT RESTRICTIONS

Apart from land restrictions, there are no other limits on foreign companies developing or owning a data centre.

Land

Prior approval from the state authority is required to lease or own land for a data centre. If the land is valued at RM 20 million (approximately US\$4.51 million) or more and the acquisition results in a reduction of Bumiputera or government agency ownership, approval from the Ministry of Economy is required (in other words, persons of the Malay race, aborigines or natives of Sabah and Sarawak).

IN PENINSULAR MALAYSIA, FOREIGNERS MUST ADHERE TO MINIMUM LAND PRICE THRESHOLDS, AND THE MAXIMUM LEASE TERM IS 60 YEARS FOR PART OF A LAND PARCEL OR 90 YEARS FOR AN ENTIRE LAND PARCEL.

Telecommunications licences

If a data centre operator is required to hold a telecommunications licence (see [Section 4](#) Telecommunications above), that licence can only be held by a Malaysian entity which typically must have a maximum of 49% foreign ownership and a minimum 30% Bumiputera equity.

06. TAX AND OTHER INCENTIVES

Special economic zones

The Johor-Singapore SEZ was formalised on 11 January 2025 to strengthen economic activity between Johor and Singapore. It consists of 9 ‘flagship areas’ including Johor Baru City Centre, Iskandar Puteri, Tanjung Pelepas-Tanjung Bin, Pasir Gudang, Senai-Skudai, Sedenak, Forest City, Pengerang Integrated Petroleum Complex and Desaru.

THE JOHOR-SINGAPORE SEZ IS DESIGNED TO FOSTER ECONOMIC COLLABORATION AND INVESTMENT BETWEEN MALAYSIA AND SINGAPORE. IT AIMS TO CREATE A VIBRANT HUB FOR BUSINESSES IN VARIOUS SECTORS, LEVERAGING THE STRENGTHS OF BOTH COUNTRIES

Tax incentives

The Malaysia Digital Economy Corporation (**MDEC**) may grant MDS to data centre developers and operators, providing access (subject to approvals and eligibility criteria) to income tax exemptions, investment tax allowances, import duty and sales tax exemptions under the Malaysia Digital Bill of Guarantees.

The Malaysia Digital Tax Incentive (**MDTI**) scheme provides reduced tax rates on qualifying income or investment tax allowances for MDS companies.

The Malaysian Investment Development Authority (**MIDA**) leads the DESAC which provides eligible ‘digital infrastructure providers’ (including data centre operators) with access to investment tax allowances of up to 100% on capital expenditure for qualifying activities (which can be offset against up to 100% of statutory income for up to 10 years) or preferential tax rates. In addition to complying with the SDDC Guidelines (see [Section 1](#) Power above), conditions for those incentives include having minimum paid-up capital, employing a minimum number of Malaysian personnel and adopting green technology.

Following the signing of the Johor-Singapore SEZ agreement between Malaysia and Singapore in early 2025, tax incentives are now available, including:

- special corporate tax rates (a special tax rate of 5% for up to 15 years for AI supply chain service businesses)
- custom incentives for businesses operating in the flagship areas (see above)
- special tax rates for knowledge workers (15% for 10 years), and
- lower entertainment duties.

Other incentives

The MIDA and MDEC established the Digital Investment Office as a central platform to facilitate digital investments and to support businesses in the MDTI and DESAC schemes.



COMPLIANCE AND RISK MANAGEMENT

07. DATA PROTECTION AND CYBER SECURITY

Data protection or privacy laws

The *Personal Data Protection Act 2010* requires data controllers (in this context, they are usually customers of data centre operators) and data processors (which may be data centre operators, depending on the services they offer) to take practical steps to protect personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction by having regard to certain factors. Data controllers and data processors must also implement technical and organisational security measures in accordance with the Security Standard set out in the Personal Data Protection Standard 2015 issued by the Personal Data Protection Commissioner (**Commissioner**).

Under the *Personal Data Protection (Amendment) Act 2024*, organisations that process personal data or sensitive personal data above the prescribed thresholds or that conduct activities that require regular and systematic monitoring of personal data, must appoint a Data Protection Officer. The officer must meet specified language, expertise and resident requirements.

In the event of a **personal data breach** which causes or likely to cause significant harm, organisations must notify the Commissioner within 72 hours from breach awareness, and affected individuals within 7 days after the notification is made to the Commissioner.

A new **right to data portability** also allows individuals to request the transfer of their data from one data controller to another (to the extent that such a transfer is technically feasible and the requested data format is compatible).

THIS MAY IMPACT CUSTOMER REQUIREMENTS FOR DATA CENTRES SUCH AS FACILITY LOCATION (SO PERSONAL DATA IS STORED IN A LOCATION SAFE FROM PHYSICAL AND NATURAL THREATS), ACCESS CONTROLS AND SECURITY REQUIREMENTS (SUCH AS CCTV COVERAGE).

Cyber security laws

Essential ICT systems and assets whose disruption could impact national security, economic stability, government operations, public safety and individual privacy are regulated as ‘national critical information infrastructure’ (**NCII**) under the *Cyber Security Act 2024*. The NCII covers a range of sectors which include (among others) ‘information, communication and digital’. It is unclear if any data centres are classified as NCII because the list of NCII is kept confidential to mitigate cyber threats.

08. CRITICAL INFRASTRUCTURE AND SECURITY

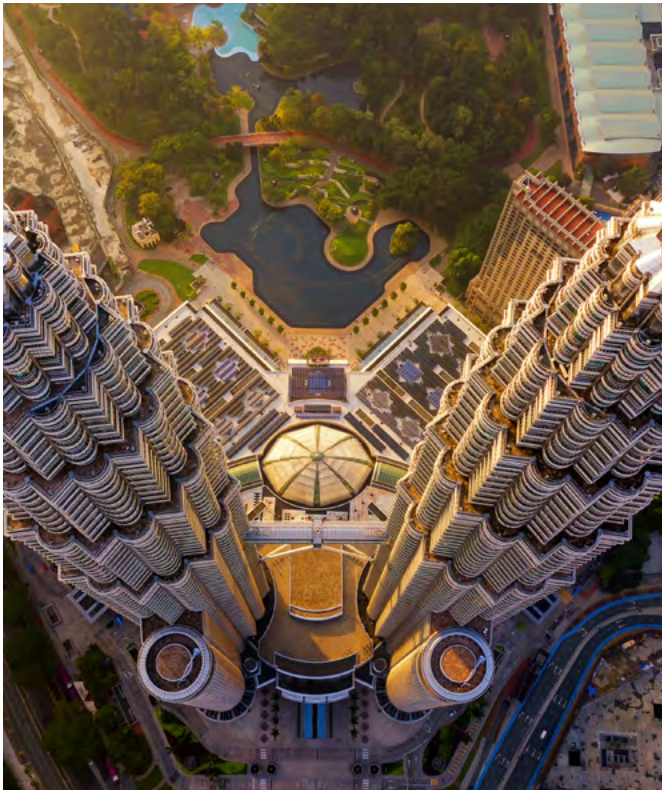
Critical infrastructure laws

See [Section 7](#) Data protection and cyber security above.

ANY DATA CENTRE OPERATOR OR DEVELOPER OF NCII MUST COMPLY WITH CODES OF PRACTICE, SECURITY CONTROLS, BEST PRACTICES, AND CONDUCT RISK ASSESSMENTS AND AUDITS.

National security issues

Data centres that store or process classified data may be designated as protected areas or places under the *Protected Areas and Protected Places Act 1959* or classified areas under the *Official Secrets Act 1972*.



09. DATA LOCALISATION

Specific data localisation obligations may apply to customers of a data centre depending on the type of data processed at the facility and the customer’s industry.

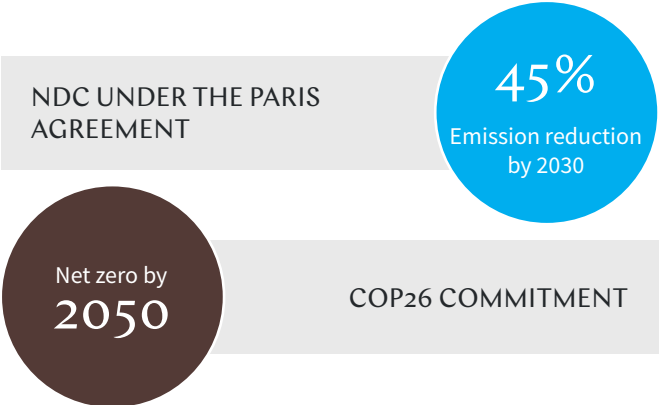
- **Highly regulated sectors**, such as financial services (see [Section 11](#) Sector-specific regulations below) and healthcare, may impose localisation requirements through industry guidelines or licence conditions. For example, copies of Malaysian tax and employment records must be kept in Malaysia.
- **Personal data laws** prohibit the export of personal data unless the data subject’s consent has been obtained or an exception applies (for example, the transfer is necessary for the performance of a contract with data subject).

10. ENVIRONMENTAL, SOCIAL AND GOVERNANCE

International ESG commitments

There is currently no federal law implementing Malaysia’s various commitments, including targeting net zero emissions by 2050. However, there are some on the way, as well as state-level regulations in place.

- The **National Climate Change Policy 2.0** outlines Malaysia’s pathway to net zero, published in 2024 by the Ministry of Natural Resources and Environmental Sustainability.
- A **Climate Change Bill** to implement Malaysia’s commitments under the Paris Agreement is in draft form.
- A **carbon tax** is set for implementation in 2026 under a commitment made in the 2025 Budget.
- States may enact their own legislation. Sarawak introduced the *Environment (Reduction of Greenhouse Gases Emission) Ordinance 2023* which regulates greenhouse gas emissions and carbon credit units in Sarawak.



ESG audits, systems and impact assessments

The *Energy Efficiency and Conservation Act 2024* requires large energy consumers (prescribed by the *Energy Efficiency and Conservation Regulations 2024* as consuming 21,600 gigajoules or more) to complete **periodic energy audits** and implement **energy management systems**.

A data centre developer may need to undertake an **environmental impact assessment** under the *Environmental Quality Act 1974* if criteria specified in the *Environmental Quality (Prescribed Activities) (Environmental Impact Assessment) Order 2015* are met relating to the physical slope or size of the development.

Handling of waste

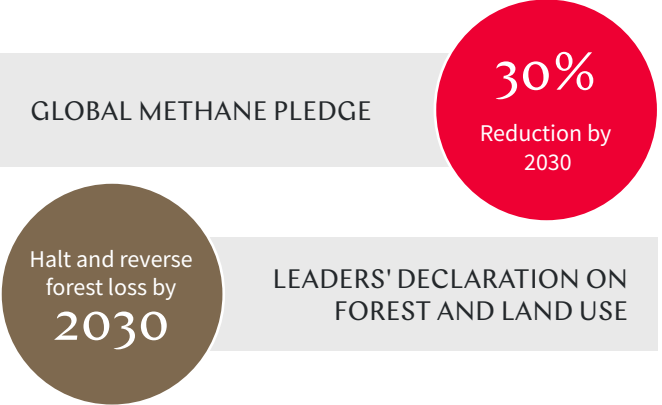
Electronic waste generated from retired servers, networking equipment and other IT infrastructure may need to be handled and treated in accordance with *Environmental Quality (Scheduled Wastes) Regulations 2005* and the *Environmental Quality Act 1974* to minimise environmental impact.

ESG reporting

Bursa Malaysia ACE Market require **listed entities** to include a statement of sustainability-related risks and opportunities in their annual reports that (among other things) accords to the International Sustainability Standards Board (**ISSB**) Standards and specifies performance against metrics and targets.

The National Sustainability Reporting Framework (**NSRF**) was published in 2024 to provide **listed and large non-listed companies** with a common language for sustainability reporting, using International Financial Reporting Standards (**IFRS**) Sustainability Disclosure Standards issued by the ISSB as the baseline, and introduced assurance requirements for sustainability reporting. The SDDC Guidelines also encourage sustainability reporting.

There are other relevant corporate governance obligations and voluntary codes to consider.



11. SECTOR-SPECIFIC REGULATIONS APPLICABLE TO DATA CENTRES

Government bodies

The Guideline for Information Security Management through Cloud Computing in the Public Service includes considerations for government agencies when using **cloud services**, such as data centre physical security controls. This was issued by the Chief Government Security Office.

Government agencies must also keep **official secrets** (defined in the *Official Secrets Act 1972*) onshore, and host specific information (such as documents concerning national security, national defence and international relations or cabinet documents) on their premises or in a government data centre.

Telecommunications operators

The Technical Code on Information and Network Security – Cloud Service Provider Selection contains requirements for organisations to follow when selecting cloud service providers, and refers to business continuity management and operational resilience in its example of a cloud control matrix. Issued by the MCMC, compliance with these technical codes is voluntary unless tied to a specific legal obligation, such as a telecommunications licence condition.

If a data controller is a telecommunications licensee, it must register as a data controller with the Commissioner and comply with the Personal Data Protection Code of Practices for the Communications Sector. This includes complying with the technical and organisational security measures that may be implemented for compliance with the Security Standard or comparable alternative measures. See [Section 7](#) Data protection and cyber security above regarding data protection and privacy.

NFP and NSP licences include network security requirements on licensees including (among others):

- to comply with network security and information integrity requirements imposed by authorities
- to ensure compliance with applicable security standards, codes, best practices, guidelines or directives relating to network reliability and integrity, and
- to design and deploy their networks to allow for effective investigation and enforcement of local laws, including by protecting against online harms and fraud. See [Section 4](#) Telecommunications above regarding telecommunications licensees.

Financial services providers or financial institutions

The Risk Management in Technology Policy (**RMIT Policy**) for financial institutions managing technology risks contains specific requirements for data centre infrastructure and operations. Issued by Bank Negara Malaysia (**BNM**), the RMIT Policy requirements include:

- resiliency, security and scalability
- redundancy for production data centres
- dedicated space for hosting critical systems
- adequate control procedures
- real-time monitoring for utilisation and system performance, and
- independent risk assessments to safeguard sensitive data.
- Boards and senior management of financial institutions are expected to exercise oversight and address risks associated with outsourcing critical technology functions and systems, including by:
 - conducting due diligence on service providers
 - establishing service level agreements with minimum requirements, and
 - ensuring service providers comply with the RMIT Policy.

The Guidelines on Data Management and Management Information System Framework (**Data Management Guidelines**) require financial institutions to establish and maintain a sound data management and MIS framework. The Data Management Guidelines outline principles for sound data management and MIS practices that financial institutions must observe relating to data governance, data and systems Infrastructure, data quality and data security and privacy.

A policy document on Management of Customer Information and Permitted Disclosures also issued by BNM outlines requirements for financial service provider’s handling of customer information.

E-money issuers

BNM requires e-money issuers to ensure that sensitive customer information is not stored offshore as a condition of their licence. See [Section 9](#) Data localisation above regarding data localisation.

Digital asset service providers

The Malaysian Securities Commission’s Guidelines on Digital Assets set regulatory requirements for Initial Exchange Offering (**IEO**) platform operators and digital asset custodians, including to maintain secure infrastructure and to ensure proper selection and oversight of service providers.



PHILIPPINES

CHAPTER 8

SNAPSHOT



The Philippines is a dynamic and emerging data centre market. The market was valued at US\$633 million in 2024 and is expected to grow at a CAGR of 20.89% to reach US\$1.97 billion by 2030. The Philippines government has also been actively promoting the development of data centres through various incentives and regulatory support, positioning the country as an attractive destination for investment.

Nevertheless, the country faces challenges such as foreign ownership restrictions and existing utility infrastructure limitations. There has been an increased focus on sustainability, and the country's commitment towards renewable energy initiatives and government support provides opportunities for growth in the data centre market.

OPPORTUNITIES

- ✓ Growing digital economy
- ✓ Government support
- ✓ Renewable energy initiatives

CHALLENGES

- ✗ Foreign ownership restrictions for land
- ✗ Infrastructure limitations
- ✗ Competition from surrounding countries

SPOTLIGHT ON KEY DRIVERS

GOVERNMENT INCENTIVES

The Philippines government offers a range of incentives to attract data centre investments, including tax holidays, tax and duty exemptions on imported items, tax credits and additional deductions.

The Philippine Economic Zone Authority monitors and evaluates the developments and requirements of ecozones (where data centres are permitted), providing a favourable environment for investment. The 2022 Strategic Investment Priority Plan (**SIPP 2022**) and the *Corporate Recovery and Tax Incentives for Enterprises Act of 2021* (**Tax Incentives Act**) also offer enhanced deductions and preferential corporate income tax rates for data centres.

RENEWABLE ENERGY AND SUSTAINABILITY INITIATIVES

The Department of Energy has set ambitious targets for renewable energy, aiming for a 35% share of renewable energy in the national electricity generation mix by 2030 and 50% by 2040.

The Green Energy Option Program (**GEOP**) allows new connections with an estimated monthly peak demand of ≥ 300 kW to source power directly from renewable energy sources. These initiatives provide data centres with opportunities to adopt sustainable practices and reduce their carbon footprint, as well as ensuring secure grid connection.

LONGER-TERM LAND LEASES

The maximum duration of long-term leases of land granted to foreign investors is expected to extend from 50 years (renewable by a further 25 years) to 99 years.

At the time of publication, a proposed bill - House Bill No. 10755 - has been passed by both the House of Representatives and the Senate. This will amend the *Investors' Lease Act of 1993* and is in the process of being finalised and sent for the President's signature.

'The Philippines is fast emerging as Southeast Asia's next data centre hotspot, driven by surging digital demand, strategic location and strong government support for digital infrastructure.'

Peter Pacheco
Partner
Romulo Mabanta Buenaventura Sayoc & De los Angeles



OPERATIONAL

01. POWER

Getting power to a site

Power supply is open to competition and there are various suppliers. The biggest suppliers (based on market share) are San Miguel Corporation, AboitizPower and First Gen. However, electricity distribution is allocated to 1 distribution utility in each franchise area. Unlike other counties in Southeast Asia, power is not subsidised in the Philippines, and the cost of power in the Philippines is the second highest in Asia, after Singapore.

Data centres must be constructed on industrial land parcels with satisfactory grid capability. With multiple suppliers over different geographical areas, the process of securing power to a site varies depending on site location, the relevant supplier’s processes and whether the power requirements can be serviced by an existing connection with the distribution utility.

- If the required power **can be provided by a distribution utility**, then the process to procure power is **straightforward**.
- **If not**, a satisfactory grid impact study may be needed before a supplier will enter into an electricity supply agreement. If a grid impact study is needed, **it can take approximately 60 days** from the date of application for a grid impact study to be conducted.

The Philippines’ biggest suppliers in an open market...

- San Miguel Corporation
- AboitizPower
- First Gen

Power purchase agreements

The Philippines’ electricity sector operates under a deregulated framework established by the *Electric Power Industry Reform Act of 2001 (EPIRA)*.

EPIRA established the Energy Regulatory Commission (**ERC**) and separates the electricity industry into 4 key activities:

- generation
- transmission
- distribution, and
- supply.

Power generation is largely privatised, with multiple independent power producers competing to supply electricity.

Transmission is managed by the government-owned National Transmission Corporation (**TransCo**), although its operations and maintenance are run by the privately-owned National Grid Corporation of the Philippines (**NGCP**).

Electricity distribution is handled by regional utilities, which are either private distribution utilities (**DUs**) or electric cooperatives (**ECs**), both regulated by the ERC. Private DUs, such as the Manila Electric Company (**MERALCO**), operate in urban and densely populated areas, while ECs provide service in rural regions. Most DUs are privately owned, while ECs are community-owned but receive government support and subsidies.

This dual system creates a fragmented regulatory environment, with varying levels of efficiency and service reliability across regions.

The competitive retail electricity market (**CREM**), introduced under EPIRA, allows large electricity consumers (500kW threshold) such as data centres to procure power directly from retail electricity suppliers rather than relying on regional utilities. This market structure, combined with programs like the GEOP, enables end-users to bypass traditional utilities and directly contract renewable energy from licensed suppliers.

HOWEVER, NAVIGATING THIS COMPLEX LANDSCAPE REQUIRES CAREFUL CONSIDERATION OF REGULATORY COMPLIANCE, GRID ACCESS, AND REGIONAL UTILITY FRAMEWORKS

Energy laws, regulations, policies and guidelines

There is currently no regulatory framework specific to powering data centres. In general, power generators sell power through bilateral contracts with DUs or ECs or sell at the Wholesale Electricity Spot Market.

Power from the generators is transmitted through transmission lines owned by the TransCo which is operated by its concessionaire the NGCP. For distribution, this is handled by private utilities within specific franchise areas. Each franchise area is monopolised by 1 DU. The ERC regulates both transmission and distribution, and reviews and approves power supply agreements, retail suppliers then serve contestable customers in the CREM.

GEOP - Green Energy Option Program

End users with a new power connection:

- that have been in operation for less than 12 months, and
- with an estimated monthly peak power demand of ≥ 300 kW

are eligible for the GEOP established under the *Renewable Energy Act of 2008*.

GEOP participants can elect to source power directly from renewable energy power sources rather than obtaining power from the franchised electricity distributor. Data centre operators not part of the GEOP can still source power directly from renewable energy power sources.

02. WATER

Water supply

Data centre developers must get a permit to obtain bulk water supply from the National Water Resources Board (**NWRB**). The application requires, amongst other things:

- proof of right to use the relevant land
- certificates of registration with the relevant agencies (for example, the Department of Trade and Industry, Cooperative and Development Authority and Securities and Exchange Commission), and
- an Environmental Compliance Certificate or Certificate of Non-Coverage from the Department of Environment and Natural Resources - Regional Office.

The application process takes a **minimum of 60 days**. Water utilities are generally available in econozones.

Water laws, policies and guidelines

Data centres may be impacted by the Philippine Water Supply and Sanitation Master Plan (**PWSSNP**), launched by the National Economic and Development Authority in 2021. The aim of the PWSSNP is to **provide universal access to safe and sustainable water and sanitation across the country by 2030** and the regulatory environment is expected to evolve to achieve this aim.

DATA CENTRES MAY BECOME SUBJECT TO STRICTER STANDARDS OR INCREASED COSTS AS INDUSTRIAL USERS DUE TO THE PWSSNP.

ELECTRICITY DISTRIBUTION REGIONAL UTILITIES - DUAL SYSTEM

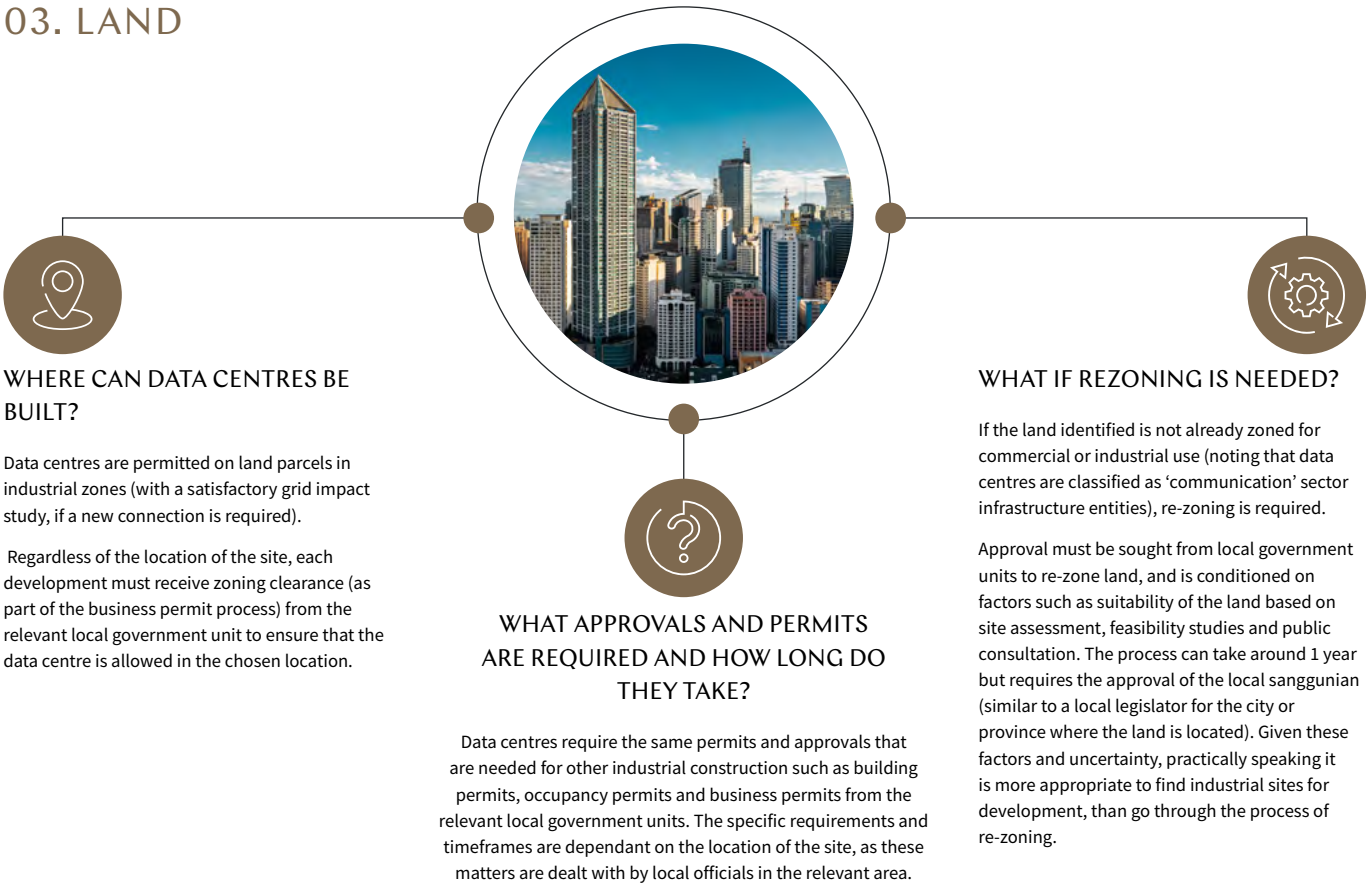


OR... data centres and other large consumers **using 500kw+ can bypass** traditional utilities...

COMPETITIVE RETAIL ELECTRICITY MARKET
DIRECT CONTRACT - RENEWABLE ENERGY FROM LICENSED SUPPLIERS



03. LAND



04. TELECOMMUNICATIONS

Is a telecommunications licence required?

A data centre operator is not required to obtain a telecommunication licence if it does not provide telecommunication services or operate its own network.

Applicability of telecommunications laws to data centres

Telecommunication laws are not applicable to data centres where the operator does not provide telecommunication services. Usually, it is the licensed telecommunication service providers who provide services to the facility that are subject to telecommunications laws.



STRATEGIC OPPORTUNITIES

05. FOREIGN INVESTMENT RESTRICTIONS

Land

Ownership of land is limited to Philippine entities with a **maximum of 40% foreign ownership**. However, foreign entities that exceed that threshold may enter into a long-term lease of land provided that they comply with the *Investors' Lease Act of 1993*.

- **Currently**, the maximum term of the long-term lease is **50 years**, with the possibility to extend (automatic renewal is not possible) for **another 25 years**.
- **Proposals** are expected to extend this to **99 years**. At the time of publication, the proposed bill has been passed by both the House of Representatives and the Senate and is in the process of being finalised and sent for the President's signature.

Water Permit

The NWRB will only grant a water permit to Philippine citizens and corporations that have **at least 60% Philippine ownership**. However, water utilities are available in economic zones.

06. TAX AND OTHER INCENTIVES

Ecozones

There are **over 400 ecozones** in the Philippines including Clark SEZ which is set to house the Narra Technology Park data centre campus. Data centres can operate in all ecozones in the Philippines. The developments and requirements of ecozones are monitored and evaluated by the Philippine Economic Zone Authority. Incentives in those ecozones are not specific to data centres and depend on the relevant ecozone.

Incentives generally include...

- tax holidays
- tax / duty exemptions on imported items
- tax credits
- additional deductions
- non-fiscal incentives such as employment of foreign nationals
- simplification of customs procedures

Tax incentives – Data centres may be eligible under the SIPP 2022 and the Tax Incentives Act for:

- **tax holidays** of 4 to 7 years duration, depending on the location and classification of the site, with longer incentives generally being granted to facilities located in an under-served region
- **enhanced deductions**, which typically include an additional enhanced depreciation allowance on capital expenditure such as buildings, machinery and equipment, and
- a **preferential corporate income tax rate** of 5% for a maximum period of 10 years from expiration of a tax holiday.

COMPLIANCE AND RISK MANAGEMENT

07. DATA PROTECTION AND CYBER SECURITY

Data protection or privacy laws

The *Data Privacy Act of 2012* requires organisations (including cloud storage providers) who handle personal data to register with the National Privacy Commission as either a Personal Information Controller (**PIC**) or a Personal Information Processor.

Data centres, and their customers, are required to appoint a Data Protection Officer if they process or control personal data and must implement appropriate organisational, physical and technical security measures to safeguard personal data.

PICs must also ensure that any third parties processing personal data on their behalf (which may include data centre operators) likewise adopt such protective measures, including data centre operators.

Cyber security laws

Operators should adhere to guidance issued by the National Privacy Commission which outlines best practices for data centre security including:

- security controls and technologies
- policies which are applicable across physical, virtual and cloud environments, and
- monitoring of the network.

Operators must also retain traffic data and subscriber information for a **minimum of 6 months** from the date of the transaction under the *Cybercrime Prevention Act of 2012* as part of the Philippines’ efforts to prevent and combat cybercrime.

08. CRITICAL INFRASTRUCTURE

Critical infrastructure laws

Data centres are currently not caught by the *Republic Act No. 11659 (Republic Act)*. This impacts foreign investment in public services which own, use, or operate systems and assets, whether physical or virtual, so vital to the Philippines that the incapacity or destruction of such systems or assets would have a detrimental impact on national security, including telecommunications and other such vital services (and which are declared by the President of the Philippines).

The Republic Act provides that if there is no reciprocity between the country of the foreign investor and the Philippines, then control over such critical infrastructure cannot exceed 50%.

09. DATA LOCALISATION

General data localisation requirements

There are no general data localisation or data residency requirements. The Philippines has however supported initiatives such as the [Asia-Pacific Economic Cooperation \(APEC\) Cross-Border Privacy Rules](#) system, which is a framework designed to enhance the protection of personal data when it is transferred across borders.

Data localisation requirements for government agencies

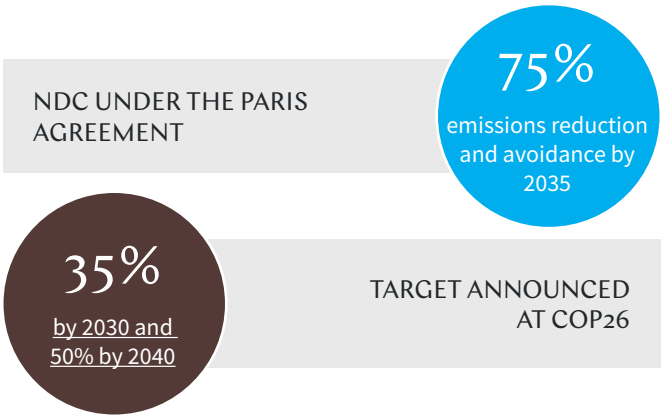
The Department of Information and Communications Technology requires all personal data processed by a government agency or by a private entity in relation to a government transaction to be localised.



10. ENVIRONMENTAL, SOCIAL AND GOVERNANCE

International ESG commitments

The Philippines is a signatory to the Paris Agreement with a NDC target of 75% by 2030. Although specific commitments have not been enacted into domestic law, the *Climate Change Act of 2009* established the Climate Change Commission which oversees and coordinates climate change policies and plans.



Power Development Plan

The Philippines Department of Energy has made a commitment towards a cleaner energy transition, and as part of that has proposed a national renewable energy electricity generation target of 35% by 2030 and an aspirational target of 50% by 2040 through the Power Development Plan 2023-2050 (**PDP**). However, the PDP is not mandatory and reflects the aspirations of the department in relation to the desired future energy mix.

ESG reporting

The Securities and Exchange Commission is in the process of implementing mandatory sustainability reporting for listed companies by 2026, through a phased approach.

Voluntary accreditation

It is not uncommon for data centres to hold international certifications, such as the EDGE certification for green buildings. For example, Digital Edge’s data centre in Manila (NARRA1 is certified with ANSI/TIA-942-C, EDGE and US LEED Gold).

11. SECTOR-SPECIFIC REGULATIONS APPLICABLE TO DATA CENTRES

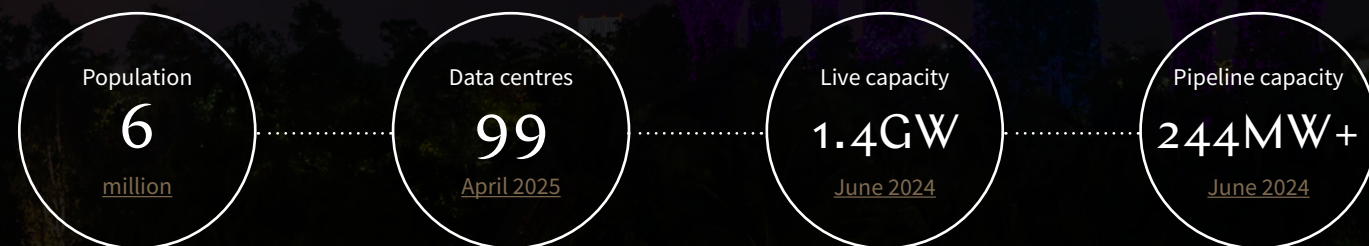
Government bodies

See [Section 9](#) Data localisation for the targeted requirements.

SINGAPORE

CHAPTER 9

COUNTRY SNAPSHOT | A REGIONAL DATA CENTRE HUB EMERGES



Singapore is the leading data centre hub in Asia, a title it has held for some time. It offers a stable, well-regulated and highly connected environment. With strong submarine cable infrastructure, 100% foreign ownership permitted and targeted tax incentives, Singapore remains a preferred regional base for hyperscalers and enterprise operators serving Asia. The government supports cross-border data flows and aligns closely with international standards, reinforcing its position as a top-tier digital infrastructure market.

However, any new development is tightly controlled under the Data Centre Call for Application (**DC-CFA**) scheme, with no rounds launched since 2023. Projects must meet strict sustainability criteria, including energy and water efficiency. Despite limited capacity, major operators continue to invest: Google completed its [fourth Singapore facility in 2024](#) (US\$5 billion total investment) and Equinix has [committed US\\$260 million to a sixth site](#) opening in early 2027.

OPPORTUNITIES

- ✓ Regional connectivity hub
- ✓ Political and regulatory stability
- ✓ Skilled workforce

CHALLENGES

- ✗ Controlled market access
- ✗ Power and land constraints
- ✗ High-cost base

SPOTLIGHT ON KEY DRIVERS

LIMITED ENTRY, HIGH STANDARDS

Following the lifting of Singapore's 2019 moratorium, the government introduced the DC-CFA scheme to regulate growth based on sustainability, strategic value and economic contribution.

However, since the pilot DC-CFA closed in 2023, no new rounds have launched, creating a temporary supply constraint. While the scheme ensures only high-impact, efficient projects proceed, it also limits new market entry. The next round is expected this year, and investors will need to act quickly when applications reopen.

DEAL, OR NO DEAL? SUSTAINABILITY AS THE DECIDER

Singapore has made sustainability a strategic priority for data centres, requiring green certifications under its Green Data Centre Roadmap.

Operators must meet strict energy efficiency, decarbonisation, and water usage standards, aligned with national environmental goals. Certification under frameworks like the BCA-IMDA Green Mark for Data Centres (**GMDC**) is increasingly expected, and green energy procurement is becoming a competitive differentiator. While these requirements may raise upfront costs, they position operators to align with both regulatory expectations and the ESG priorities of global tenants and investors.

POWER AND LAND CONSTRAINTS

Despite Singapore's advanced infrastructure, data centre growth is constrained by limited land availability and tight power allocations.

These factors result in long lead times for approvals and grid connections - particularly for high-capacity facilities. Investors must plan for competition in securing resources and may increasingly look to nearby regions like Johor and Batam for spillover capacity.

'Singapore remains the hyperconnected data centre hub for Asia. While its capacity won't grow as fast as Johor, Sydney, Tokyo, or Seoul, the allure of Singapore endures as the 'square mile' for data centre finance and capability. Its geographical limitations are being addressed with spillover options in the 'Singapore Plus' regions of Johor and Batam, while sustainability and network security are focal points for mainland Singapore.'



Daryl Cox
Partner
King & Wood Mallesons

OPERATIONAL

01. POWER

Getting power to a site

Singapore’s electricity transmission and distribution networks are owned and operated by SP Group, a government-owned entity. SP Services Ltd, a subsidiary of SP Group, manages grid connections and customer services. Data centre operators can either:

- purchase electricity at wholesale prices from SP Group, the default supplier for large businesses, or
- contract with licensed retailers such as Geneco, Keppel Electric, PacificLight or Sembcorp Power.

Operators classified as contestable consumers (being those with an average monthly electricity consumption of at least 2,000 kWh) may also register as Direct Market Consumers to buy power directly from the wholesale electricity market.

To secure a connection, applications must be made through a Licensed Electrical Worker (**LEW**). Estimated lead times are 26 months for a new 66kV connection to an existing substation, and 28 months where a new substation is required.



Rationing in supply emergencies

The *Energy Transition Measures and Other Amendments Act 2024* empowers the Energy Market Authority (**EMA**) to ration power in the event of a supply emergency, underscoring the need for resilient and energy-efficient infrastructure.

Power purchase agreements

Singapore’s electricity sector operates under a fully liberalised market framework regulated by the **EMA**. Power generation is privatised with different generators operating their own power plants. Electricity is sold to the Singapore Wholesale Electricity Market, where generators compete to supply power that can be bought by retailers or contestable customers.

The grid is owned and operated by SP Group entity that oversees transmission and distribution.

The combination of the current licensing requirements and the lack of a wheeling regime make it difficult to structure physical corporate PPAs other than for onsite solar rooftop projects. For this reason, corporate PPAs tend to be entered into as virtual corporate PPAs.

Evolutions in Singapore's ability to procure green energy, notably through import from Malaysia, mean that data centre operators may be able to procure green electricity through a custom PPA with a retailer. They should expect this to come at a premium, although this may decrease as the new import projects (and the associated interconnections to other countries) are developed and commissioned.

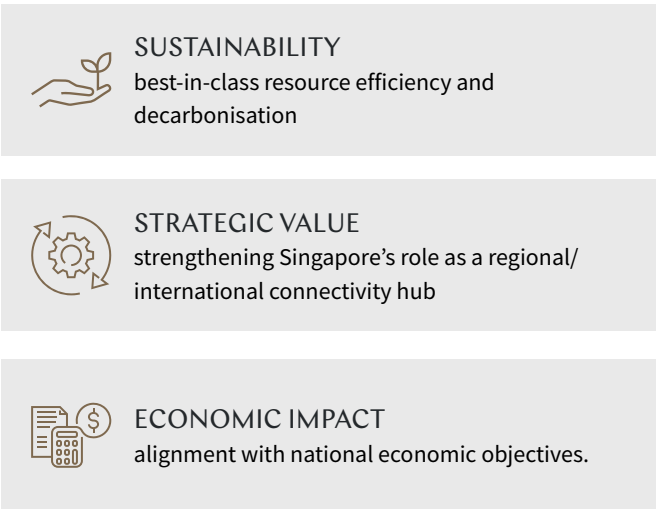
Green Data Centre Roadmap

Sustainability guidelines are set out in the [Green Data Centre Roadmap](#) published by the Infocomm Media Development Authority (**IMDA**). This covers key areas such as energy efficiency, renewable energy use and water efficiency. In addition, Singapore promotes the adoption of voluntary sustainability standards:

- SS 546:2013 (Green Data Centres – Energy and Environmental Management Systems) which sets out best practices for energy and environmental efficiency, and
- SS 697:2023 (Deployment and Operation of Data Centre IT Equipment in Tropical Climates) which promotes energy savings through higher operating temperatures.

Sustainability-led approach under pilot scheme

In 2022, Singapore lifted its 3 year moratorium on new data centre developments, adopting a selective, sustainability-led approach through the IMDA's Green Data Centre Roadmap. New data centre projects must be approved under the DC-CFA scheme administered by IMDA and the Economic Development Board though, as at July 2025, no new rounds have launched since 2023. The DC-CFA evaluates proposals based on:



Applicants to the pilot DC-CFA were required to achieve platinum certification – the highest tier with the most stringent standards – under the GMDC certification scheme, suggesting that future applicants will have to meet the same standard.

See also [Section 3](#) Land below.



02. WATER

Water supply

Data centres in Singapore must secure water supply from the Public Utilities Board (**PUB**), the national water agency. Key considerations include:

- developers are required to submit water demand projections and may need to install private meters, or implement water recycling systems to meet efficiency targets
- water usage, especially for cooling, is closely monitored, and PUB may impose water efficiency benchmarks
- applications typically proceed alongside other utility clearances and can take 3 to 6 months, depending on project scale and complexity. Early engagement with PUB is recommended to ensure alignment with sustainability and infrastructure requirements.

Water efficiency and other requirements

The IMDA, in collaboration with PUB, aims to achieve a WUE of 2.0 m³/MWh or lower over the next decade.



03. LAND

Securing land

Most industrial land in Singapore is held on a **leasehold basis**, with terms typically ranging from 60 to 99 years. Shorter leases of 30 or 60 years may apply in government-managed estates (such as those under JTC Corporation (**JTC**)). Lease terms and conditions are shaped by the timing of land release, zoning rules and the specific land-use scheme.

JTC oversees major industrial estates and business parks including Changi Business Park, Jurong Innovation District, Punggol Digital District and Tanjong Kling. Tanjong Kling serves as a dedicated data centre park.

Subletting without JTC’s prior approval is not permitted. Unauthorised subletting has been an ongoing concern for JTC, with 400 confirmed cases reported in 2020. However, ‘service providers’ (which explicitly includes data centre services) **are exempt** if they have formal agreements with customers (for example, colocation customers) whose onsite presence supports the lessee’s business.

Permits and approvals

All new data centre developments in Singapore must go through the DC-CFA scheme, administered by IMDA and the EDB. The timing and availability of DC-CFA exercises are set by the government. The pilot round concluded in July 2023, with the next round expected in 2025.

- Developers must secure general land development approvals such as planning permission and building plan approvals.
- Timelines for securing permits, licences and approvals vary significantly and there is no standard timeframe - depending heavily on project complexity, government processes, environmental assessments and the need for technical consultations, the process can range from a few months to over a year.

What ‘Green Certification’ is available?

Developers can obtain the GMDC which certifies that operators have successfully deployed green data centre best practices, demonstrating superior sustainability and environmental performance in a data centre (see [Section 1](#) Power above). The GMDC is awarded on a facility-by-facility basis and rates performance against key areas such as energy efficiency, sustainable design and construction, use of digital tools and maintainability.

Where can developers build data centres – and is re-zoning possible?

Data centres in Singapore can be developed on land zoned ‘Business 2 (Industrial)’ and, in some cases, ‘Business 1 (Industrial)’ or ‘Business Park’.

All developments require planning permission from the Urban Redevelopment Authority (**URA**), which assesses proposals with relevant technical agencies to ensure compliance with zoning, environmental, and infrastructure requirements. The URA’s Master Plan is reviewed periodically and may result in zoning changes.

While there is no formal rezoning process specific to data centres, developers may apply for a change of use for existing properties to support re-zoning requests.

04. TELECOMMUNICATIONS

Is a telecommunications licence required? It depends...

A telecommunications licence is generally only required where a data centre provider:

- provides telecommunication services (for example, IP transit) to external customers, or tenants,
- operates or owns infrastructure (such as fibre, switching equipment) used to deliver telecommunication services to third parties, or
- resells or provides telecom services over leased infrastructure.

Operators that only offer **infrastructure hosting**, such as colocation or private network support for customers, generally fall outside the licensing regime.

Data centres **offering connectivity or network services** may require licensing from the IMDA as Facilities-Based Operators or Services-Based Operators. Licensees must comply with specific licence conditions, such as quality-of-service standards, restrictions on establishing telecommunication links outside their premises and adherence to advisory guidelines.

Data centre operators that **manufacture, import, sell, lease or offer for sale** any telecommunications equipment in Singapore must obtain a Telecommunications Dealer’s Licence under the *Telecommunications (Dealers) Regulations*.

STRATEGIC OPPORTUNITIES

05. FOREIGN INVESTMENT RESTRICTIONS

Singapore actively promotes foreign investment and generally permits 100% foreign ownership across most sectors, including data centres and cloud service providers. There are no specific restrictions on foreign ownership in the sector. Importantly, foreigners and foreign-owned companies can lease industrial land (see [Section 3](#) Land above).

However, the government now has the authority to screen investments in **entities deemed critical to national security**, under the *Significant Investments Review Act 2024*. While no data centre operators have been designated to date, those with strategic or infrastructure significance could fall within scope, though the regime is expected to apply narrowly and on a case-by-case basis with low impact on most commercial data centre investments.



06. TAX AND OTHER INCENTIVES

Special economic zones

Singapore does not operate designated SEZs. However, its pro-investment environment, strong infrastructure and policy stability continue to attract data centre investment. A key regional development is the Johor-Singapore Special Economic Zone, formalised on 11 January 2025. Located in Johor, Malaysia, this bilateral initiative aims to deepen cross-border trade, investment, and digital integration. For more details, see [the Malaysia chapter](#) of this guide.

Tax incentives

Singapore offers a range of tax incentives to encourage data centre investment and sustainable operations, which include:

- **Pioneer Certificate Incentive:** Provides corporate tax exemptions or reduced rates for 5 to 15 years on income from qualifying activities.
- **Data centre operators may qualify if** they introduce advanced technologies, skillsets or know-how that significantly exceeds prevailing industry standards in Singapore. Examples might include high-efficiency cooling systems, AI-enabled energy optimisation or cutting-edge security infrastructure.
- **Development and Expansion Incentive:** Offers a reduced corporate tax rate - as low as 5% or 10% - on income derived from manufacturing activities for companies expanding or upgrading business activities in Singapore.

This is particularly relevant for data centre operators that are building new data centres, upgrading existing facilities or scaling up regional operations.

- **Low corporate tax rate:** A competitive base rate of 17%, among the lowest in the region, enhancing Singapore’s attractiveness as a regional data centre hub.
- **Green Incentives:** Companies investing in energy-efficient technologies or green-certified data centres between 31 March 2021 and 31 December 2026 may qualify for income tax deductions under various green investment schemes.

Other incentives

The EDB and National Environment Agency (**NEA**) offer several non-tax incentives to support energy-efficient and green data centre investments, including:

- **Investment Allowance for Emissions Reduction:** Additional capital allowances for qualifying projects that reduce GHG.
- **Energy Efficiency Grant:** Co-funding support for energy-efficient equipment and retrofitting by the NEA, up to 70% support for pre-approved equipment.
- **Resource Efficiency Grant for Emissions:** Support for projects that improve energy and carbon efficiency in industrial operations, based on corresponding support rate for the carbon abatement achieved, capped at 50% of qualifying costs.

These schemes aim to lower the upfront cost of sustainable infrastructure and encourage long-term environmental performance.



COMPLIANCE AND RISK MANAGEMENT

07. DATA PROTECTION AND CYBER SECURITY

Data protection or privacy laws

Data centre operators must comply with the *Personal Data Protection Act 2012 (PDPA)* when handling or processing personal data on behalf of Customers? – bearing in mind that those requirements are more likely to be relevant to customers of the operators’ services. The PDPA includes:

- obligations to implement **reasonable security measures** to protect computer systems and prevent unauthorised access and
- restrictions on **cross-border transfers** of personal data unless the receiving party ensures a comparable level of protection.

Cyber security laws

CII-classified data centres must comply with mandatory requirements under the *Cybersecurity Act 2018 (Cyber Act)*. This includes:

- **Implementing cyber security safeguards**, conducting audits and risk assessments, reporting incidents and following codes of practice issued by the Commissioner of Cybersecurity (**Commissioner**)
- **Operational resilience obligations**, including establishing a cyber security governance framework, maintaining an up-to-date inventory of CII assets, implementing safeguards and developing incident response and recovery plans.

Resilience guidelines (set to become mandatory)

The Cyber Act is complemented by the IMDA’s Advisory Guidelines for Resilience and Security of Data Centres (**IMDA Guidelines**), which aim to strengthen data centre resilience and security.

These voluntary guidelines recommend practices such as vulnerability testing, role-based access control and maintaining a robust business continuity management system.

The IMDA Guidelines are expected to become mandatory under the forthcoming *Digital Infrastructure Act (DIA)*, which will introduce a more comprehensive regulatory framework for data centre security and resilience in Singapore. See [Section 8](#) Critical infrastructure and security below.

While not mandatory, data centre owners are encouraged to adopt technical standards such as the Multi-Tier Cloud Security framework, TR 62 (cloud outage response) and SS ISO/IEC 21878:2019 (business continuity for cloud services).

08. CRITICAL INFRASTRUCTURE AND SECURITY

Critical infrastructure laws

In Singapore, data centres designated as CII by the Commissioner are subject to the Cyber Act.

CII owners must **safeguard systems** against cyber threats by sharing system and cyber security information with the Commissioner, complying with codes and directions, conducting audits and risk assessments, participating in exercises and reporting incidents.

The regime was broadened to reflect evolving digital threats (by the *Cybersecurity (Amendment) Act 2024*). This extended obligations to **virtualised and third-party-owned CIIs**, introducing Foundational Digital Infrastructure for critical services like cloud and data centres, and enabling the Commissioner to regulate entities supporting overseas essential services or digital supply chains.

Non-compliance with these CII obligations can result in significant penalties, including fines of up to S\$500,000 or 10% of the entity's annual turnover in Singapore, whichever is higher.

Separately, the IMDA Guidelines outline best practices to mitigate risks from misconfiguration, cyber threats, and physical hazards. These measures include risk assessments, business impact analysis, business continuity planning and cyber security measures. While currently voluntary, these measures are expected to become mandatory under the incoming DIA.

This new legislation will establish a **more comprehensive framework** for digital infrastructure resilience, going beyond cyber risk to address broader concerns such as supply chain vulnerabilities and service availability.

The DIA is expected to apply to a wider range of infrastructure, including both public and private sector data centres critical to Singapore’s digital economy. As at July 2025, specific details of the DIA have not been released, but it is anticipated to be tabled in Parliament later in 2025.

National security issues

Data centres designated as CII under the Cyber Act are required to comply with standards issued by the Cyber Security Agency of Singapore (**CSA**). This includes implementing cyber security and physical protection measures, maintaining disaster recovery and business continuity plans, and reporting cyber security incidents. Operators must also adhere to codes of practice and may be subject to regular audits and risk assessments.

Physical security issues

The GMDC includes physical security and resilience requirements, such as fire suppression systems, CCTV coverage and protection against fire, humidity, electrical faults, and lightning. It also addresses maintainability, including access for façade inspection and servicing.

Separately, under the *Infrastructure Protection Act 2017*, data centres located within or near sensitive or high-security sites (such as government facilities) may be subject to additional physical protection requirements, including security-by-design features integrated into building plans.

09. DATA LOCALISATION

Singapore does not impose general data localisation requirements. Data can be transferred and stored outside of Singapore, as long as the transfer complies with the PDPA.

10. ENVIRONMENTAL, SOCIAL AND GOVERNANCE

International ESG commitments

Singapore is a signatory to key international climate agreements, having ratified the Paris Agreement in 2016, the UNFCCC in 1997 and the Kyoto Protocol (including its second commitment period) in 2021. However, its NDC commitments have not been codified into domestic law.

Carbon tax on big emitters

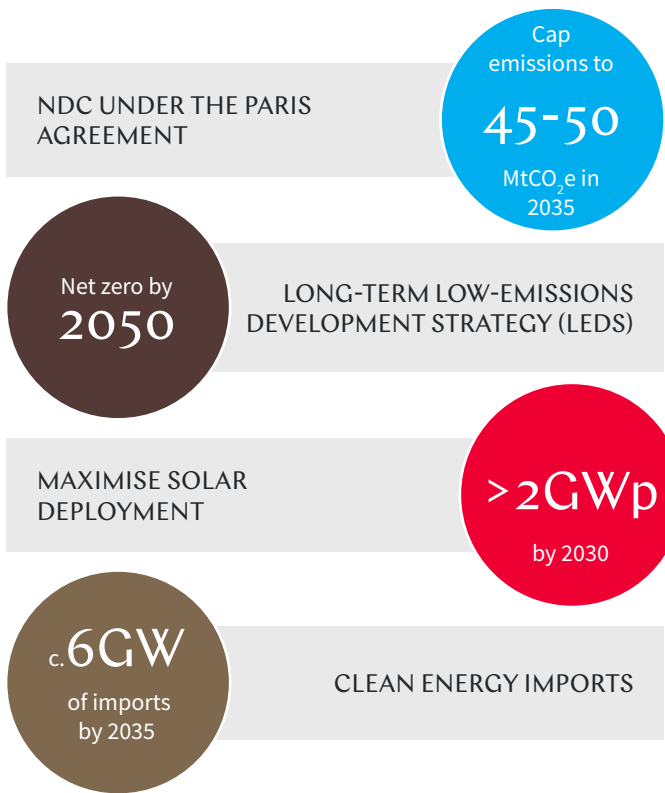
Singapore imposes a carbon tax on facilities that emit 25,000 tonnes or more of CO₂e annually.

ESG reporting

All listed companies in Singapore must file annual climate-related disclosures with the Accounting and Corporate Regulatory Authority and the Singapore Exchange regulator (SGX RegCo). This is the first milestone in Singapore’s Climate Reporting and Assurance Roadmap, aimed at boosting the city-state’s global business hub status.

Mandatory reports are required for all listed issuers from financial years starting on or after 1 January 2025.

This requirement will also [apply to large non-listed companies](#) - defined as those with annual revenue ≥ S\$1 billion and total assets ≥ S\$500 million (unless an exception applies) - for financial years starting on or after 1 January 2027.



11. SECTOR-SPECIFIC REGULATIONS APPLICABLE TO DATA CENTRES

Financial services providers and financial institutions

Engaging data centre services may subject financial institutions to obligations under the Monetary Authority of Singapore’s (**MAS**) Guidelines on Outsourcing, including risk management and audit rights.

The MAS Technology Risk Guidelines further advise financial institutions to conduct threat and vulnerability assessments of their data centre arrangements. These guidelines highlight considerations such as physical access controls, diversified data communication paths and redundant cooling infrastructure to ensure operational resilience and data security.

Digital asset providers

Digital asset providers, regulated under the *Payment Services Act* and *Securities and Futures Act*, must:

- implement business continuity and disaster recovery planning, in line with MAS Guidelines on Risk Management Practices, and
- maintain secure technology infrastructure with appropriate cyber security measures, in line with MAS Technology Risk Management Guidelines.

Where such providers outsource functions to data centre operators, they must ensure that the operators comply with the same regulatory obligations.



SOUTH KOREA

CHAPTER 10

SNAPSHOT



South Korea is a burgeoning hub for data centre investment. With its robust economy and reputation as a regional 'safe haven', it attracts strong interest from international investors, developers and operators. It presents a compelling landscape for data centre investment, particularly due to the absence of foreign investment restrictions and presence of attractive incentives.

However, potential investors must navigate challenges. Key among them are the significant electricity supply constraints and regulatory complexities. While the promise of an open and thriving economy is enticing, understanding the regulatory nuances and addressing infrastructure limitations are crucial for successful investment in South Korea.

OPPORTUNITIES

- ✓ Generally no foreign investment or ownership restrictions
- ✓ Incentives

CHALLENGES

- ✗ Lack of power supply and long lead times
- ✗ Regional water shortages and contamination risks due to monsoons and floods

SPOTLIGHT ON KEY DRIVERS

OPEN TO FOREIGN INVESTMENT

While the market is still somewhat inward looking, South Korea has a liberal approach to foreign investment and ownership offering an advantage for international investors.

There are few restrictions on land acquisition, except in designated military zones, and no specific limitations on data centre ownership — aside from a cap on foreign shares in facility-based telecommunications services.

POWER CONSTRAINTS

South Korea's power supply constraints pose a significant challenge for data centre investment and development.

Korea Electric Power Corporation (**KEPCO**) is the sole electricity provider, and it faces limitations in transformers and transmission infrastructure, particularly in high-demand areas. This bottleneck means a power procurement timeline of several years, and can lead to further delays in securing adequate power supply, complicating project timelines and operational planning. Regulatory requirements for power system impact assessments and energy use plans also add layers of complexity.

INCENTIVES IN DESIGNATED AREAS, FOR INVESTMENT ENTITIES AND FOREIGN ENTITIES

Special Opportunity Development Zones and Leading Investment Districts provide reductions or exemptions from corporate income tax and acquisition tax for data centres developed in those areas.

These zones are designed to attract foreign investment and foster innovation, creating an environment conducive to growth. Acquisition, corporate income and property taxes may also be reduced or waived if certain investment vehicles are used to invest in data centre operations. Foreign investments of over US\$2 million to develop or operate data centres involving new growth technologies, may also see similar incentives.

'Korea's new government, which took office in June 2025, is strategically positioning AI data centres as core infrastructure for national economic development. Its proactive support for attracting large-scale data centres and AI initiatives will be an opportunity for companies looking to invest in AI data centres and seeking growth and innovation.'



Jin Ho Song
Senior Attorney
Kim & Chang

OPERATIONAL

01. POWER

Supply vs demand imbalance

KEPCO is the sole electricity supplier under the *Electric Utility Act*. KEPCO faces challenges in responding to recent increases in demand and developing its infrastructure to adapt to new trends and patterns (including the growth of the data centre sector). This has led to a significant amount of land banking in areas that benefit from existing infrastructure with available capacity.

DEVELOPERS SHOULD COMPLETE DUE DILIGENCE ON THE STATUS OF ELECTRICITY INFRASTRUCTURE (INCLUDING SUB-STATIONS WITH AVAILABLE BAYS) BEFORE SETTLING ON A SITE AND MAKING COMMITMENTS TO CUSTOMERS, LANDLORDS AND CONTRACTORS.



NOTICE TO KEPCO

Data centres that need > 5MW of electricity must give notice to KEPCO in advance of requiring power

Current lead times - between 1 to 4 years



POWER SYSTEM IMPACT ASSESSMENT

Required if usage will exceed 10MW

Ministry of Trade, Industry and Energy (**MOTIE**) and KEPCO may approve or reject the power system impact assessment or may issue mandatory improvement measures

Approval is needed before applying for a building permit

Non-compliance can result in corrective or suspension orders



ENERGY USE PLAN

Data centre developers must also submit an energy use plan to MOTIE before installing the facility (under the *Energy Use Rationalisation Act*) where

For a **public operator** (that is, the State, local government or public institutions), where:

- the fuel and heat use exceeds 2,500 tonnes per annum, or
- electricity use exceeds 10 million kWh per annum

For **all other operators**, where

- the fuel and heat use exceeds 5,000 tonnes per annum, or
- electricity use exceeds 20 million kWh per annum



APPLICATION TO KEPCO

After completing the above, an application can be submitted to KEPCO

KEPCO usually takes around **3 to 6 months to review and approve** an electricity use application and enter into an electricity use agreement with the user – the actual timeframe may vary depending on the volume of required electricity, technical difficulty of reviewing the power supply plan and scale of line construction needed for the power supply

Power purchase agreements

KEPCO has a monopoly on the sale of electricity and largely dominates electricity sales. Corporate PPAs have existed since 2021 in:

- **trilateral form** - KEPCO intermediates between the consumer and generator, and
- **bilateral form** - direct agreement between generator and consumer.

These are subject to a number of regulations that require the inclusion of mandatory terms in contracts (and for KEPCO, the use of its standard terms). To be eligible to procure electricity under a corporate PPA, a consumer must have a connection of 300kVa or more.

One of the key limitations of this system is that, currently, RECs cannot be issued under a corporate PPA. Virtual corporate PPAs can be used, and a small number were reportedly signed in the past few years.

The PPA scheme is expected to become more diverse in South Korea in the future.

IN THE FUTURE, IT IS EXPECTED THAT POWER TRANSACTIONS BETWEEN GENERATORS AND CONSUMERS WILL TAKE PLACE DIRECTLY IN AREAS DESIGNATED AS SPECIALISED DISTRICTS FOR DISTRIBUTED ENERGY OR AREAS WHERE TRANSMISSION RESTRICTIONS ARE IMPOSED.

Renewable energy certificates

As in many jurisdictions in Asia, RECs are available in South Korea. The Renewable Energy Center of the Korea Energy Agency recently amended the Korean REC system. Data centre operators utilising renewable energy may find REC purchases a viable means of renewable electricity procurement.

Reducing concentration risk via distribution schemes

Most generation capacity (including nuclear) is on the east of the country, distant from the concentration of data centres in metropolitan Seoul. A significant plan to alleviate this mismatch was announced by the Ministry of Trade, Industry, Regional Integration and Employment (**MOTIE**) in March 2023, resulting in the *Special Act on Activation of Distributed Energy (Distributed Energy Act)*. In force since June 2024, the Distributed Energy Act aims to align power consumption areas with power generation areas.

The Distributed Energy Act mandates:

- the installation of distribution energy regimes
- a power system impact assessment regime for data centres that will use 10MW or more of power (as outlined above)
- a requirement for data centres to have facilities that generate some of their required power, and
- data centres in metropolitan Seoul that use over 200,000MWh of energy annually to source at least 2% of their annual energy from distributed energy (renewable energy of 40MW or more, fuel cells and other sources).

The 2% minimum will apply until 2026, **increasing to 20% after 2040**, with interim progressive targets of:

- 5% - 2027-2029
- 10% - 2030-2034, and
- 15% - 2035-2039.



02. WATER

K Water is the government agency responsible for providing both public and industrial water in South Korea.

South Korea faces significant barriers to water supply in certain provinces.

For example, in the Jeolla province, as recently as 2023, the two main reservoirs ran dry, forcing residents to rely on water trucks to supply water. In other areas, heavy monsoons and floods created contamination issues.



03. LAND

Securing land

South Korea has a separate treatment of land and building ownership interests and a dual registration system (that is, a land registry and a building registry) and there are other areas where data centres are not permitted (see over page). The land and building registries cover ownership and encumbrances (including mortgages, security interests and superficies) of relevant land parcels and buildings, respectively.

- **Registration of title under the land registry** is generally required to perfect a transfer of title to real estate (except for transfers that arise by operation of law) and, while it does not guarantee ownership of the relevant real property, registration operates as a strong presumption that the registered owner listed in the land registry is the true owner.
- **Applications for registration of transfer** of ownership must be filed jointly by the purchaser and seller.



Where can data centres be built?

Data centres are permitted in some areas, permitted with local government approval in other areas and there are other areas where data centres are not permitted. The *National Land Planning and Utilisation Act (National Land Planning Act)* is prescriptive as to the areas within which data centres can be developed.

STATUS	APPLICABLE ZONING AREAS
Permitted	Quasi-residential areas, central commercial areas, general commercial areas, neighboring commercial areas, quasi-industrial areas, productive green areas (4 floors or less), natural green areas (4 floors or less) and planning management areas (4 floors or less).
Not Permitted	Type-1 exclusive residential areas, type-2 exclusive residential areas, green areas for conservation and natural environment conservation areas.
Permitted with relevant local government ordinance	Type-1 general residential areas (4 floors or less), type-2 general residential areas, type-3 general residential areas, distribution business areas, exclusive industrial areas, general industrial areas, preservation management areas (4 floors or less), production control areas (4 floors or less) and agriculture and forestry areas.

The Ministry of Land, Infrastructure and Transport also has the power under the *National Land Planning Act* to designate district unit planning zones and impose specific zoning restrictions within those zones. This power may be used at the request of an applicant, of if the need arises to allow development for a particular use, in a certain area.

What if there are location-based restrictions, or requirements?

The *Mountainous Districts Management Act*, *Protection of Military Bases and Installations Act* and the *Landscape Act* impose building restrictions on specific sites (for example, restrictions on height, floor area ratios and building coverage ratios), restrictions on the types of facilities that can be built and sale or leasing restrictions. Developers must consider these as a part of their due diligence on a proposed site.

If land is located within an **industrial complex** and qualifies as an industrial facilities zone under the *Industrial Cluster Development and Factory Establishment Act (Industrial Complex Act)*, the entity seeking to occupy and operate a data centre must enter into an industrial complex occupancy agreement with the manager of the industrial complex and comply with applicable laws and regulations including the Industrial Complex Act.

The Industrial Complex Act requires, amongst other things, occupants to be engaged in certain qualified business activities and to directly operate on the relevant site for a certain period of time before engaging in any leasing activities.

What approvals are needed and how long do they take?

Developers must obtain development and building permits from local government, with additional permits needed if the relevant zoning is not appropriate, as noted above.

If the application is straightforward, it will generally take **between 3 to 6 months** to obtain development and building permits for a data centre development. Depending on the specifics of the site, assessments such as building committee reviews, environmental and traffic impact assessments, and landscape reviews may also be required.

There is an administrative process around commencing construction. This is not burdensome, but it means that construction can only commence after a construction commencement report is filed. Once construction is complete, an occupancy permit is also needed before the data centre can commence operation.

Dealing with neighbourhood issues

Given the nature of the facilities, civil complaints from residents are common in connection with data centre developments and have the potential to significantly delay project timelines.



04. TELECOMMUNICATIONS

Applicability of telecommunications laws to data centres

Data centre operators are classified as value-added telecommunications service providers (**VSP**) under the *Telecommunications Business Act (TBA)*. This means they must comply with the TBA and file a VSP report with the Minister of Science and ICT. A VSP report includes, amongst other things:

- a description of the services provided
- a network diagram, and
- a confirmation letter for personal information processing.

Is a telecommunications licence required?

If a data centre operator seeks to offer facility-based telecommunications services, like providing internet connectivity to its customers, a facility-based telecommunications service provider registration may be required.

Dark fibre

While it is customary for data centre operators and major customers to procure active fibre services to their facilities, dark fibre is not widely available or utilised in the South Korean data centre market ('dark fibre' is the supply of optical fibre strands or pairs, allowing customers to attach their own active equipment and control the network).



STRATEGIC OPPORTUNITIES

05. FOREIGN INVESTMENT RESTRICTIONS

Land

In general, foreign ownership of land is allowed. However, certain zoning regulations may restrict a foreigner's acquisition of land. For example, if land is designated as a military installations protection zone under the *Protection of Military Bases and Installations Act*, a foreign individual or a South Korean entity with foreign ownership of 50% or more may be restricted from acquiring it. Prior approval from the relevant local government is required.

Installation of facilities such as telecommunication, electricity, industrial and power, will be restricted if in a military installations protection zone, unless approval of the relevant military base is obtained.

Data centres

There are no specific foreign investment restrictions or domestic ownership requirements directly applicable to data centres. However, if a data centre business qualifies as a facility-based telecommunications provider - such as when it operates its own circuit (for example, via dark fibre) - foreigners may not own more than 49% of the data centre (subject to exceptions that apply based on the nationality of the investors and the overall investment structure).

06. TAX AND OTHER INCENTIVES

Special Opportunity Development Zones, Leading Investment Districts and other location-based incentives

- **Special Opportunity Development Zones** have been established as part of efforts to attract large-scale corporate investment in non-metropolitan areas outside of Seoul. These offer tax incentives by way of a reduction or exemption from corporate income tax and acquisition tax for a certain period.
- **Leading Investment Districts** have also been established, offering similar incentives to Special Opportunity Development Zones if minimum investment and employee thresholds are met. The purpose is to foster growth hubs or invigorate private investment within the relevant area.

The 'Hydrothermal Energy Convergence Cluster' in the Gangwondo province has been designated as a Leading Investment District to create a data centre cluster using hydrothermal energy. The Gangwondo province already houses data centres for Naver and Samsung SDS.

- **Local incentives** are provided by numerous municipal governments (Jeonlanamdo, Gyeongsangbookdo, Jeonlabookdo) to attract data centre investments, which includes investment subsidies, discounted rent or long-term leases.
- **Foreign investment zones** provide reductions in acquisition and property tax if a foreign invested enterprise:
 - occupies the zone with a minimum foreign investment, and
 - operates a data centre business.

The Guidelines for Operation of Foreign Investment Zones outline three foreign investment zones: complex, service-based and individual zones. There are currently more than 100 foreign investment zones, with many in Gyeonggi, Busan, Incheon, Ulsan and Gyeongnam. The minimum foreign investment to receive tax benefits varies by industry, and is US\$30 million for computer programming, system integration and management.

Tax incentives

- **Investment vehicles**

Investment vehicles like a Real Estate Fund (**REF**), Real Estate Investment Trust (**REIT**) and Project Financing Vehicle (**PFV**) can take advantage of corporate income tax rate reductions or exemptions in certain circumstances when they construct a new data centre without directly operating the facility (for example, if they lease the data centre to an operator).

Acquisition and property tax benefits may also apply depending on where the investment vehicle is established. Generally speaking, real estate acquired in the Seoul Metropolitan Area, or by an entity established, or with a branch, in the Seoul Metropolitan Area, attracts a higher acquisition tax rate. However, REFs, REITs and PFVs that are established in the Seoul Metropolitan Area are not subject to that higher rate when they acquire real estate in the Seoul Metropolitan Area.

- **Foreign investors**

Foreigners that invest \$US2 million or more and develop or operate a data centre that involves new growth technologies (for example, data centre cooling, air conditioning and energy efficiency technology), may benefit from acquisition tax and property tax reductions and exemptions even if the investment is made outside of the Special Opportunity Development Zones or Leading Investment Districts.



COMPLIANCE AND RISK MANAGEMENT

07. DATA PROTECTION AND CYBER SECURITY

Data protection or privacy laws

All data centre operators who **operate their facility for third party customers** (including colocation, hosting, cloud and circuit-lease services) must obtain Information Security Management System (**ISMS**) certification, under the *Network Act on Promotion of Information and Communications Network Utilisation and Information Protection (Network Act)*. This certifies that information security related measures and activities meet prescribed standards. Certification is not required when the data centre is for captive use (that is, serving the operator’s own internal systems) unless the data centre operator has:

- generated ≥ ₩10 billion (US\$6.8 million) in revenue from the information and communication service sector in the previous year, and
- an average daily domestic user count of ≥ 1 million over the last 3 months, as at the end of the previous year.

Data centre operators that provide **cloud services or infrastructure as a service to public institutions** must hold Cloud Security Assurance Program (**CSAP**) certification under the *Electronic Government Act* and relevant guidelines. CSAP certification requires the separation of facilities for public institutions from those for others, which may affect a data centre’s structure.

Cyber security laws

ISMS and CSAP certification also relate to cyber security. The standards include implementing measures to address infringement incidents and security measures to prevent unauthorised access.

08. CRITICAL INFRASTRUCTURE AND SECURITY

Critical infrastructure laws

• Critical Information Infrastructure (CII)

The government may designate telecommunication facilities, such as data centres, as CII under the Act on the *Protection of Information and Communications Infrastructure (PICI Act)*.

The CII-designated facilities in the telecommunications sector currently include facilities for internet connection services, mobile phone/internet services, internet exchange services, Voice over Internet Protocol services and Internet Protocol Television services. The CII-designated facilities may include data centres that support these types of service providers.

The CII designation process is government-initiated. The Ministry of Science and ICT will choose to initiate an assessment process which considers:

- national and societal importance of the facilities
- the degree of dependence of the management organisation on these facilities, and
- the scale and scope of potential damage in the event of a security incident to determine whether to make a designation.

Operators of CII must regularly assess vulnerabilities, implement management measures, and provide notifications and remedies to affected individuals upon infringement incidents.

• Critical Telecommunications Facilities

‘Large-scale’ data centres are classified as critical telecommunications facilities, requiring disaster management plans under the government’s annual guidelines (*Framework Act on Broadcasting Communications Development*), if they have:

- either:
 - computer rooms of clustered information and communications facilities of 22,500m² or more, or
 - facilities of 40MW or more in power intake capacity, **and**
- annual revenue exceeding ₩10 billion (US\$6.8 billion).

National security issues

Networks, devices and facilities used in data centres used by the government and public institutions may undergo a Security Review by the National Intelligence Service (**NIS**) under the Electronic Government Act.

In January 2025, NIS released a draft ‘Security Guideline for National Network Security Framework’, detailing the security measures required before a security review request. NIS plans to implement these guidelines in the second half of 2025.

Physical security issues

Under the Network Act, data centre operators must implement protective measures (including access control for visitors and measures to protect the facilities and equipment in a disaster situation) when facilities are:

- provided to customers and have ≥ 500m² floor area of white space, or
- for captive use and they have:
 - ≥ 500m² floor area of white space
 - generated ≥ ₩10 billion (US\$6.8 million) in revenue from the information and communication service sector in the previous year, and
 - an average daily domestic user count of ≥ 1 million over the last three months, as at the end of the previous year.

Given the low thresholds, most data centres are caught by this requirement.

The *Framework Act on Intelligence Informatisation* requires data centres to be equipped with specific facilities such as whitespace, computer rooms and emergency power generation facilities.



09. DATA LOCALISATION

Targeted or indirect data localisation requirements

While South Korea has no general data localisation requirements, there are several targeted data localisation requirements:

• Cloud service providers operating in the public sector

Cloud service providers must obtain a CSAP certification to operate in the public sector under the *Electronic Government Act*. CSAP certification requires cloud systems, data processing and data to be physically located in South Korea.

‘The CSAP, which applies to Korea’s central, provincial and local public sector with very limited exceptions, creates significant barriers to foreign cloud service providers seeking to sell to South Korea’s public sector.’

- United States Trade Representative, [2025 National Trade Estimate Report on Foreign Trade Barriers](#)

The Foreign Trade Barriers report cites the need to ‘create physically separated facilities for exclusive use by government’ and ‘create backup systems and data’. However, in September 2024, NIS waived the local encryption algorithm requirement up to the mid-tier CSAP certification. There are further requirements on CSAP certified organisations described in [Section 7](#) Data protection and cyber security above.

• Financial institutions

Under the *Electronic Financial Transactions Act*, financial institutions must locate a system processing unique identification information or personal credit information in the course of using cloud services within South Korea.

• Healthcare professionals and hospitals

The *Medical Service Act* prohibits healthcare professionals and hospitals from storing any electronic medical records outside of South Korea.

• National information

Data centres that possess or manage and seek to export any ‘national core technology’ to a foreign entity are required to file a report with, and obtain prior approval from, MOTIE under the *Act on Prevention of Divulgence and Protection of Industrial Technology*. For the purposes of national core technology, it relates to industrial technology which, if leaked, may have a detrimental effect on national security and the development of the national economy.

Further, digital map data from the National Geographic Information Institute (**NGII**) cannot be transferred overseas, unless approved by the NGII (*Act on Establishment and Control of Geospatial Information*).



10. ENVIRONMENTAL, SOCIAL AND GOVERNANCE

International ESG commitments

South Korea is a signatory to the Paris Agreement. The *Framework Act on Carbon Neutrality and Green Growth for Coping with Climate Crisis* (**Carbon Neutrality Act**) regulates greenhouse gas emissions and enshrines the NDC of a 40% reduction in greenhouse gas emissions by 2030 in comparison to 2018 levels.

NDC UNDER THE PARIS AGREEMENT

40%
emissions reduction
by 2030

Net zero by
2050

DECLARED AT THE
G20 SUMMIT IN 2020



Read about the government's extensive decarbonisation efforts, including plans to establish hydrogen cities and transform industrials under its Green New Deal, in KWM's Navigating The Net Zero Transition guide.

ESG laws, regulations and guidelines

Under the *Carbon Neutrality Act*, companies whose annual average total GHG over the last 3 years is > 50,000 metric tons of carbon dioxide equivalent (**tCO₂eq**), or which have at least one place of business where the annual average of GHG of > 15,000 tCO₂eq, must:

- set an emissions reduction target
- follow that target by reducing their emissions, and
- report to government on emissions annually.

This applies to all industries including data centres. Beyond this general requirement, South Korea has no data centre specific regulations for ESG.

11. SECTOR-SPECIFIC REGULATIONS APPLICABLE TO DATA CENTRES

Government bodies

Data centres used by the government may be subject to CSAP certification and NIS security review under the *Electronic Government Act* (see [Section 7](#) Data protection and cyber security and [Section 9](#) Data localisation above).

Financial services providers or financial institutions

Under the *Electronic Financial Transactions Act* and the *Electronic Financial Supervision Regulation* (**EFSR**), data centres used by South Korean financial services providers and financial institutions engaging in electronic financial business need to satisfy the IT room requirements as specified under the EFSR.

Virtual Asset Service Providers

The *Act on Reporting and Using Specified Financial Transaction Information* requires a Virtual Asset Service Provider (**VASP**) to file a VASP report to the Korea Financial Intelligence Unit of the Financial Services Commission.



TAIWAN

CHAPTER 11

SNAPSHOT



Taiwan is emerging as a prime data centre market in the APAC region. As a global leader in semiconductor innovation, with ongoing efforts to encourage the growth of high-tech industries, Taiwan is a reliable and strategic location for investment. Hyperscalers such as Microsoft, Google and Oracle have an established presence.

Power supply issues have led to restrictions on development in certain locations, and a growing trend of heightened scrutiny and regulation of foreign investment add regulatory complexity to the sector.

Yet for all its challenges, Taiwan's data centre market is poised for growth, powered by innovation, forward-looking government approaches and sustainable practices.

OPPORTUNITIES

- ✓ Innovative tax incentives
- ✓ Modern land zoning regime

CHALLENGES

- ✗ Foreign investment restrictions
- ✗ Power supply issues in some regions

SPOTLIGHT ON KEY DRIVERS

ADVANCED TECHNOLOGY LEADER

Taiwan excels in advanced technology research and manufacture, sitting 9th overall in the IMD World Digital Competitiveness Ranking. This is in large part due to Taiwan's dominance in the global semiconductor market.

The Taiwan Semiconductor Manufacturing Company recorded a 65% share of the wafer foundry market across July to September 2024, producing over 90% of the world's most advanced semiconductors.

Google and Microsoft have leveraged this by establishing AI research and development bases in Taiwan. More recently, in May 2025 Nvidia unveiled a partnership with Foxconn to build an AI factory in Taiwan.

POWER SUPPLY ISSUES LEADING TO SUSTAINABLE GROWTH

Taiwan's strategic approach to power supply ensures sustainable growth in the data centre sector, balancing targeted development with environmental responsibility.

The Taiwan government is restricting power supply for data centre developments in Taoyuan City and northern regions of Taiwan in response to power supply issues in these areas.

At the same time it is encouraging development in the middle and southern regions of Taiwan where power supply is more stable and there are more renewable sources. Coupled with Taiwan's commitments to renewable energy and sustainability, this represents a considered and forward-looking approach for the sector.

INCENTIVISING INNOVATION

To further strengthen Taiwan's position as a leader in innovation, the *Statute of Industrial Innovation* promotes investment through targeted tax incentives.

These are directed at smart machinery, mobile communications and new hardware, software, technology or technical services related to information security products or services. This growth in advanced industries has, in turn, increased demand for data centre development.

'Taiwan's strategic push to become a regional data hub is accelerating, driven by the regulatory framework, renewable energy initiatives and increasing demand for AI infrastructure. Legal and compliance frameworks are evolving in step with this rapid development.'

Janice C. H. Lin
Partner
Tsar & Tsai Law Firm



OPERATIONAL

01. POWER

Getting power to a site

The sole electricity provider in Taiwan is the state-owned power company, Taiwan Power Company (Taipower). To obtain supply from Taipower, data centre developers with contracted capacity of over 1MW or area over 10,000m² must first obtain Taipower’s approval for their facility’s electricity usage plan and grid connection requirements.

When the electrical usage plan and grid connection requirements have been approved, an application can be submitted, and construction of any power facilities must be carried out in accordance with design plans approved by Taipower.

Following completion of construction and on-site inspection by Taipower, approval will be granted and power supply will commence. The timing for this process varies.

It may take between 6 months to 1 year for the electrical usage plan to be approved and the application completed. Timing depends on the on the availability of Taipower’s grid and power supply capacity, the location of the facility and any complexities in power facility design.

Generally, Taipower will supply on its standard terms and conditions rather than entering into a standalone with electricity users.

How to obtain supply

The process for data centre developers with contracted capacity > 1MW or area >10,000m²



Obtain approval

must first obtain Taipower’s approval for their facility’s electricity usage plan and grid connection requirements



Submit application

to Taipower



Construction of power facilities

carried out in accordance with design plans approved by Taipower



Completion and on-site inspection

undertaken by Taipower



Approval granted

for start of power supply

Power purchase agreements

While developers often enter into supply arrangements with Taipower on standard terms, developers can also source electricity through corporate PPAs.

If the developer and renewable electricity generator are connected to the grid, developers can execute corporate offsite physical PPAs. Under this structure:

- Taipower will, as the grid operator, ‘wheel’ the electricity generated by the generator
- the generator must comply with:
 - the applicable laws (such as the *Energy Business Act*, *Electricity Business Registration Regulations* and *Renewable Energy Development Act*), and

- Taipower’s rules to obtain the necessary licenses, consents, permits and approvals from Taipower, the electricity regulator and other competent authorities to supply electricity through the corporate PPA.

There are no statutory thresholds or caps. The contents of the corporate PPA itself are negotiable.

AS OF 2025, CORPORATE PPAS WITH CAPACITIES RANGING FROM 10MW (SOLAR PV SOURCE) TO 900MW (OFFSHORE WIND SOURCE) HAVE BEEN REPORTED.

Efforts to manage supply

Taipower can amend its rules, guidelines and practices to maintain the stability of the grid and power supply (under the *Electricity Business Act*). Taipower has used this power recently in a bid to curb demand where it outstrips supply and channel it to other areas.

- **Taoyuan City and northern regions restricted:** In August 2024, it was reported that Taipower will no longer approve electricity usage plans for new data centres **with a contracted capacity of ≥ 5MW** to these areas. This practice has been adopted due to insufficient power supply in those regions and to encourage more data centre developments in the middle and southern regions of Taiwan where there is more stable power supply, more renewable power sources and less demand.
- **Price hikes:** Taipower and the Ministry of Economic Affairs (MOEA) reviews electricity prices on a yearly basis. In April 2024, as part of nation-wide structured hikes impacting all electricity users, Taipower’s price of power supplied to data centres with an electricity consumption volume of ≥50,000MWh increased by 15% to 25%.

Requirement for renewable source

Electricity users with a contracted capacity of ≥ 5MW in the previous year are currently required to source 10% of its annual contracted capacity in the previous year from renewable energy. This is under the:

- *Renewable Energy Development Act (REDA)*, and
- *Regulations for the Management of Setting up Renewable Energy Power Generation Equipment of Power Users above a Certain Contract Capacity (Renewable Energy Regulations)*.

The REDA also establishes a general aim of securing 27GW of power supply from renewable energy by 2025. This is reviewed on a rolling basis.

On 2 May 2025, MOEA issued a release in relation to a recent review and it is now estimated that 20% of power in the electricity market will be supplied by renewable energy by November 2026, with this aiming to reach 30% by 2030.

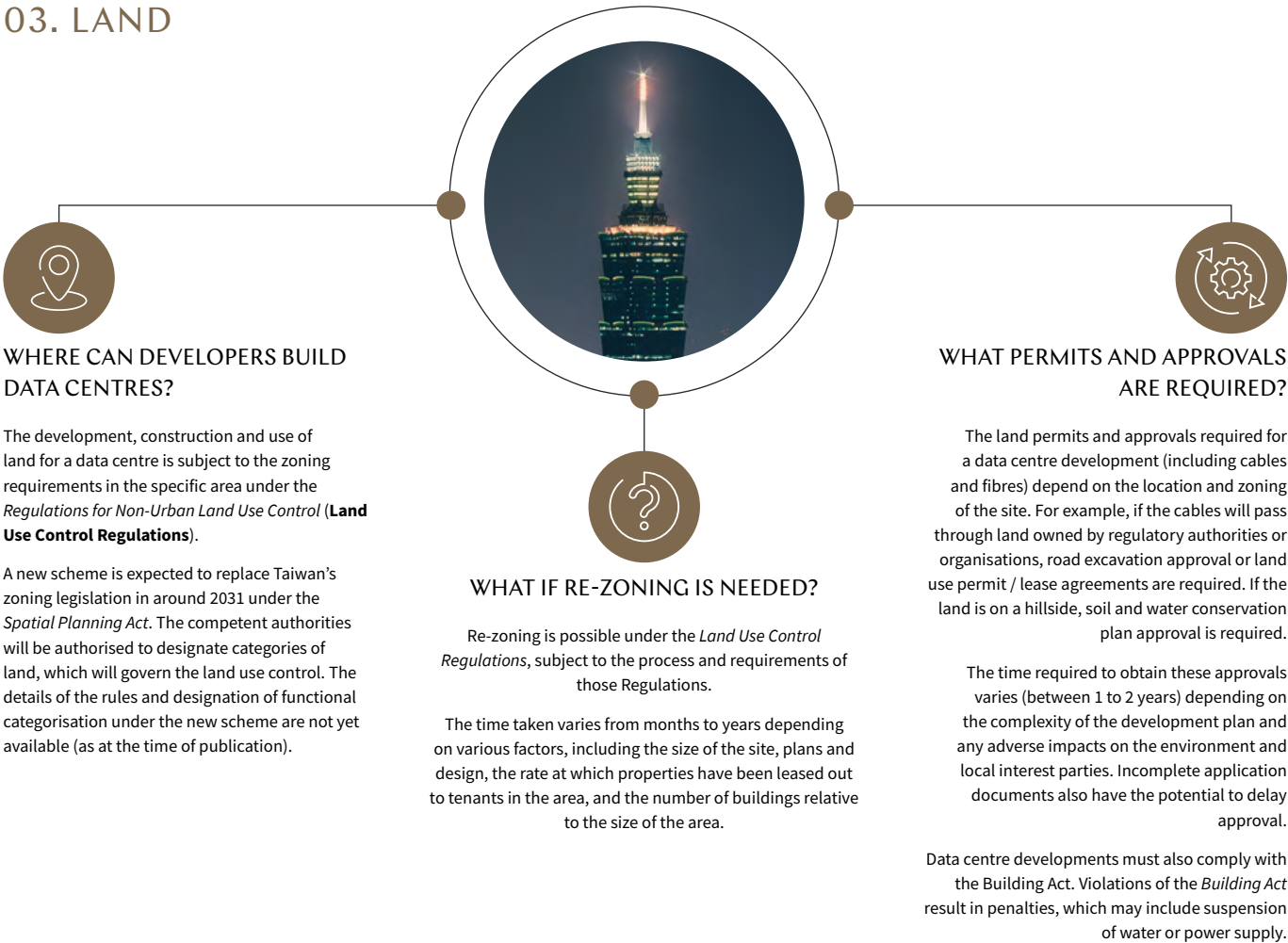
02. WATER

Water supply

Water is supplied by Taiwan Water Corporation (TWC). An application for supply needs to include a water facilities construction plan, and an on-site inspection is required before water supply will commence. Approval for the runoff control plan may be required under the *Water Act* and relevant regulations depending on the type and the size of the relevant site. For example, if the development area is two hectares or more, a runoff control plan will be required.



03. LAND



04. TELECOMMUNICATIONS

Applicability of telecommunications laws to data centres

The *Telecommunications Act* only applies to data centres if the data centre services involve 'telecommunications', which the Act states to include:

'convey, transmission or reception of signs, signals, writing, pictures, sounds or messages of any other nature in a wire or wireless manner through the use of optical, electromagnetic systems, or other scientific products'.

Data centre operators do not typically engage in the services that involve 'telecommunications' under the *Telecommunications Act*.

Is a telecommunications licence required?

Only if the data centre developer, or operator, is supplying a telecommunications service. For example, where a data centre is solely providing colocation services, a telecommunications licence is not required.

STRATEGIC OPPORTUNITIES

05. FOREIGN INVESTMENT RESTRICTIONS

Land

Foreigners may acquire and lease land through a locally incorporated company. However, the *Land Act* prohibits foreigners and foreign entities from **directly acquiring or leasing** certain land (for example, fishery lands and land with mineral deposits).

Taiwan authorities also have the power to designate that foreign acquisition of certain land are subject to an application and approval process.

Data centres

Foreign investment into a data centre **may be restricted** under:

- the *Statute For Investment By Foreign Nationals*, which applies to non-PRC foreign investors (**foreign investment regulations**), and
- the *Regulations Governing the Permission of Investment by Nationals in Mainland Area*, which prohibits direct and indirect PRC investment in any data centre (**PRC investment regulations**).

All inbound investment requires a **prior application** to the Department of Investment Review (**DIR**) of the MOEA, which oversees both regimes.

Under its **foreign investment regulations**, Taiwan imposes restrictions on foreign investment in specific industries under a 'negative list'. For example, foreign investment is:

- completely prohibited** in industries such as weapons manufacturing and postal services, and
- restricted** in industries such as telecommunications (which may apply to data centres, see [Section 4](#) Telecommunications above), and subject to increased scrutiny from Taiwanese authorities.

Taiwan authorities can also restrict, prohibit, or impose conditions on the investment for reasons such as **national security**.

Investors from PRC are subject to more restrictions than investors from other countries. Under its **PRC investment regulations**, Taiwan only allows investments from PRC investors on a 'positive list' of industries. A PRC investor is generally considered to be:

- an entity (individual, organisation or institution) of mainland PRC (**mainland person**), or
- any company that:
 - has more than 30% of its shares/ownership structure held, or
 - is substantially controlled, directly or indirectly, by a mainland person.

The 30% shareholding rule applies at each level of ownership for an organisation, or institution. There are also further restrictions on foreign investments that may have political or military affiliations with the PRC.

Similar to the foreign investment regulations, even where foreign investment from a PRC investor is approved, Taiwanese authorities may impose restrictions and conditions. However, as noted above, PRC investors are prohibited from investing (directly or indirectly) into a data centre in Taiwan.

06. TAX INCENTIVES

Special economic zones

The *Statute of Industrial Innovation* allows an investor to credit a percent of its investment against income tax. This incentive aims to spur investment in the AI industry, which could boost data centre demand. It applies to investments in:

- new smart machinery
- 5G mobile communication systems, and
- new hardware, software, technology or technical services related to information security products or services.

The amount that can be credited will depend on the year(s) during which the credit is applied and is subject to certain caps (in respect of this credit, and in aggregate with other investment credits).



COMPLIANCE AND RISK MANAGEMENT

07. DATA PROTECTION AND CYBER SECURITY

Data protection or privacy laws

The *Personal Data Protection Act (PDPA)* requires private enterprises to adopt appropriate data protection measures.

The PDPA also authorises authorities to designate certain sectors or private enterprises as being required to establish and implement personal data security and safety maintenance plans.

Different requirements apply depending on the designated sectors, groups and data types. For example, **businesses in digital economy industries have been deemed as a designated sector** under the *Regulations Regarding the Security Maintenance and Administration of Personal Information Files in Digital Economy Industries* (2023) (**Digital Economy Industries Regulations**).

Under these Regulations, regulated businesses are required to have a security and maintenance plan which addresses, among other things:

- data security management measures
- procedures for handling personal data, and
- incident prevention, reporting and response mechanisms.

This can result in data centre operators being required to adopt back-to-back cyber safety measures to ensure compliance with their customers' regulatory requirements.

Cyber security laws

The *Cyber Security Management Act (CSMA)* requires government agencies and designated critical infrastructure suppliers to meet certain cyber security safety liability levels and implement cyber security maintenance plans. This can result in data centre operators being required to adopt back-to-back cyber safety measures.

08. CRITICAL INFRASTRUCTURE AND SECURITY

Critical infrastructure laws

Under the CSMA, physical or virtual assets, systems or networks which may have a significant impact on:

- national security
- social and public interests
- people's lives, or
- economic activities,

if their functions cease to operate, or the performance of which are reduced, are regulated as critical infrastructure (**CI**).

Guidance issued by the Executive Yuan categorises energy, water resources, telecommunications, transportation, banking and finance, emergency aid and hospitals, central and local governments and high-tech parks as CI.

A telecommunications facility is regarded as critical facilities or systems supporting:

- **telecom services**, such as domestic/long distance/ international telecommunications, mobile telecommunications, satellite telecommunications, international marine cables and data telecommunications, or
- **communication services**, such as wireless broadcasting television and cable broadcasting television.

Data centres may be considered to be CI if they are a telecommunications facility or support any of these sectors and are designated as such by the sector's relevant competent authority.

Operators of CI must comply with cyber security measures based on the size, area and substitutability of its operations, and the potential impact caused if disrupted. CI is subject to regular inspection by Taiwanese authorities.

National security issues

Any foreign (including PRC) investment that may have an adverse impact on national security is prohibited under both the foreign investment regulations and PRC investment regulations (see [Section 5](#) Foreign Investment Restrictions above).

The PDPA also provides authorities with the power to issue rulings restricting certain industries from transferring certain data to particular jurisdictions if there are national security concerns (see [Section 9](#) Data Localisation, below).

09. DATA LOCALISATION

Targeted localisation requirements

While there is no general data localisation or data residency requirement in Taiwan, the PDPA provides authorities with the power to restrict the international transfer of personal data (including sensitive data) in instances where:

- major national interests are involved
- an international treaty or agreement so stipulates
- the country receiving the personal data lacks proper data protection laws and the data subjects' rights and interests may be compromised as a result of the off-shore transfer, or
- the cross-border transfer of the personal data to a third country is carried out to circumvent the PDPA.

Prohibitions on certain PRC transfers of data

In 2012, the National Communications Commission announced a ruling prohibiting the **cross-border transfer of personal data** to the PRC by any Taiwanese telecommunications business, on the grounds that the PRC personal data protection laws are inadequate. This does not explicitly apply to data centres, but will apply to data centres that are governed by the *Telecommunications Act*.

In 2022 and 2023 the Ministry of Health and Welfare and Ministry of Labor respectively announced a ruling prohibiting **social worker offices and human resources agencies** from transferring their service targets' personal data to the PRC for the same reason.

The Medical Record Regulations also require that data of **medical institutions** must be stored only in Taiwan (see [Section 11](#) Sector-Specific Regulations, Medical Institutions below for more information).



10. ENVIRONMENTAL, SOCIAL AND GOVERNANCE

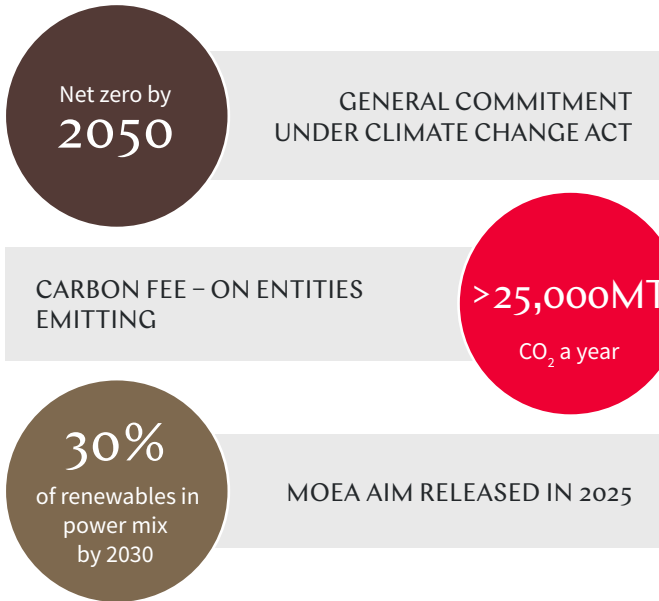
International ESG commitments

Taiwan is not a signatory to any international ESG commitments, but the Taiwan government has leveraged international conventions such as the United Nations Framework Convention on Climate Change as a reference for domestic laws to implement domestic ESG commitments.

Domestic targets and the ‘carbon fee’

The *Climate Change Response Act (Climate Change Act)* establishes a general commitment to achieve net zero by 2050 and introduces a carbon fee regime.

The regime applies to entities that emit over 25,000 metric tons of CO₂ equivalent per year and would include a data centre that exceeds this threshold. More generally, it will also capture fossil-fuel based power plants and the semiconductor and electronics manufacturing, steel and cement industries.



Environmental requirements

The *Energy Administration Act* includes various energy consumption related requirements, including power saving objectives and measures, reporting requirements (see below) and requirements for the design and construction of new buildings to meet power saving standards.

If the business of a data centre involves or generates water, soil, groundwater or air pollution or waste, it will be subject to environmental laws such as the:

- *Water Pollution Control Act*
- *Soil and Groundwater Pollution Remediation Act*
- *Air Pollution Control Act, or*
- *Waste Disposal Act*

Environmental Laws

Under these Environmental Laws, an operator may be subject to requirements relating to reporting and disclosure, environmental permits, waste disposal, or liability (depending on the type and level of pollution).

In some instances, a data centre development may be required to obtain an **environmental impact assessment approval** under the *Environmental Impact Assessment Act*. Whether or not this is required depends on various factors such as the voltage of any substations and the location or size of the development area.

ESG reporting for large energy consumers and listed companies

Energy users (including data centres) with a contracted capacity > 800kW must report their **energy consumption data** annually to the MOEA under the *Energy Administration Act*. A draft amendment to the *Energy Administration Act*, published in July 2024 proposes that names of violators of the *Energy Administration Act* will be reported to the public, but that has not yet passed as at the date of this report.

Taiwan listing laws also require **listed companies** to disclose ESG matters (including carbon emission reduction objectives) in their financial statements, have sustainable development goals and prepare sustainability Guide.



11. SECTOR-SPECIFIC REGULATIONS APPLICABLE TO DATA CENTRES

Government bodies

Except in exceptional circumstances, government bodies are required to establish their own data centres rather than lease private data centres.

Telecommunications operators

Data centres established by a licensed telecommunication enterprise are subject to the following regulations (depending on the service provided), which set out the details of the establishment and management of businesses providing the relevant services:

- *Regulations on the Management of Fixed Communication Services, or*
- *Regulations for Administration of Mobile Broadband Businesses.*

Financial services providers or financial institutions

The:

- *Regulations Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operation, and*
- *Self-Regulation Guidelines for Financial Institutions' Outsourcing of Operations to Cloud Services*

require financial institutions and financial service providers, in their outsourcing contracts with cloud service providers, to specify the scope of the outsourcing arrangements and the responsibilities of the service provider. As an example, this includes clearly delineating key obligations and rights like data ownership and audit access.

Medical institutions

The *Medical Institution Electronic Medical Record Creation and Management Regulations* designate medical institutions as a key infrastructure supplier and impose certain requirements for cloud services provided to medical institutions. This includes that the data of medical institutions must be stored only in Taiwan and that service providers must pass certain cyber security standards.



THAILAND

CHAPTER

12

SNAPSHOT | INVESTOR-FRIENDLY MARKET WITH STRATEGIC ADVANTAGES

Population

71

million

Data centres

42

April 2025

Live capacity

510MW

2024

Pipeline capacity

400MW+

Feb 2025

Thailand's data centre market is relatively small compared to other APAC countries, with an estimated value of US\$1.56 billion in 2024. However, it offers promising potential, supported by relatively simple regulatory frameworks and affordable capital requirements. Economic and tax incentives, including special economic zones and economic corridors, support data centre development and foreign investment through corporate tax exemptions, land ownership rights and streamlined approvals.

While Thailand is generally investor-friendly, it faces the same pressures as other APAC countries in managing sustainable growth. In response to growing global demand, it has introduced initiatives to accelerate the adoption of renewable energy.

OPPORTUNITIES

- ✓ Affordability
- ✓ Simple regulatory framework
- ✓ Exemptions for foreign ownership restrictions

CHALLENGES

- ✗ Regional competition

SPOTLIGHT ON KEY DRIVERS

THE FUTURE IS RENEWABLE

As Thailand advances toward a more sustainable future, the Energy Regulatory Commission (ERC) has implemented key initiatives.

These are aimed at enabling 100% renewable energy use in data centres. Specifically, the ERC has introduced the first stage of the Utility Green Tariff program and a Direct Power Purchase Agreement (DPPA) scheme, offering data centre operators the opportunity to purchase renewable energy:

- at premium rates, and
- directly, from producers.

INCENTIVES, INCENTIVES, INCENTIVES

Thailand offers a range of incentives to attract data centre investment, which have already drawn major players such as ST Telemedia Global Data Centres and Amazon Web Services.

These include dedicated SEZs and financial incentives designed to support large-scale digital infrastructure.

- **With over 15 SEZs near ports and transport hubs**, these areas offer logistics, connectivity, and resources ideal for data centres. In particular, the Eastern Economic Zone is being earmarked as Thailand's 'Silicon Valley'.
- **General and sector-specific benefits** are provided by the Board of Investment (BOI), including corporate income tax and VAT exemptions.

NO DATA CENTRE-SPECIFIC REGULATION FOR WATER OR ZONING

Thailand does not impose data centre-specific regulation on water supply or zoning, with developments subject only to standard utility and land use rules.

This regulatory flexibility lowers barriers to entry, making Thailand an attractive destination for data centre investment.

Water supply for data centres in Thailand is not specifically regulated and is managed by the relevant utility providers or local water authorities.

Similarly, data centre developments are subject to standard land and zoning requirements, with no special permits needed.



'Strong investment growth in Thailand's data centre industry is fuelled by digital transformation in the private and public sector. Thailand's stable energy supply, internet speed, land availability and strategic location in Southeast Asia, supported by Government incentives, make it an attractive destination for investors.'

Jessada Sawatdipong
Chairman and Senior Partner
Chandler Mori Hamada

OPERATIONAL

01. POWER

Getting power to a site

The Electricity Generating Authority of Thailand (**EGAT**) is a state-owned utility enterprise which maintains a monopoly on electricity transmission in Thailand. The EGAT sells electricity on a wholesale basis to the Metropolitan Electricity Authority (**MEA**) and the Provincial Electricity Authority (**PEA**). The MEA is responsible for electricity distribution to end users within Bangkok metropolitan areas, while the PEA is responsible for electricity distribution to end users for the rest of Thailand.

Data centre operators **must procure power from either the PEA or MEA by entering into a PPA**. This process typically takes around 30 business days but may vary depending on site-specific factors.

Power purchase agreements

Aside from procuring supply from the PEA or MEA, developers may enter corporate onsite physical PPAs. These are typically used for rooftop solar installations. Although there are some examples of large, utility scale (10MW+) onsite rooftop solar PPAs, they are developed on industrial facilities with a large horizontal footprint and may not be an adequate source of supply for data centres.

The availability of corporate offsite physical PPAs is, at the time of publication, still limited, although recent policy announcements signal this may change in the future. For example, the National Energy Policy Council has announced a **direct PPA pilot scheme** with a quota of up to 2GW which is expected to be reserved to certain data centres.

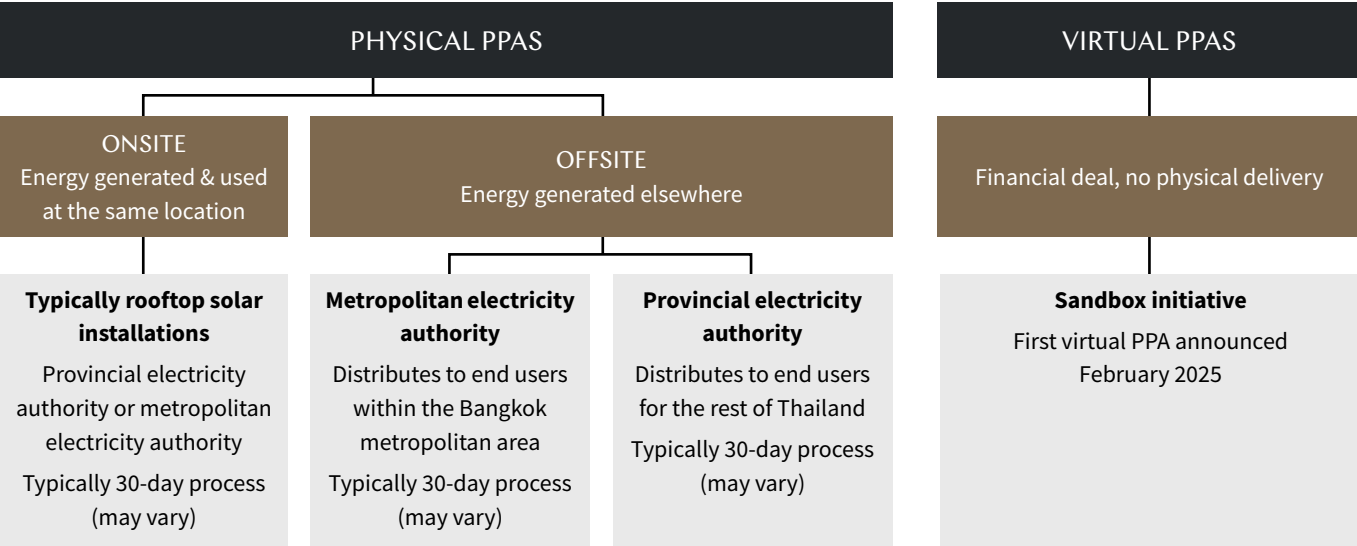
For this to be effective, it is expected that the government, the electricity regulator and the 3 entities dealing with electricity transport and distribution (EGAT, PEA and MEA) will need to finalise third party access codes which they have been developing in the last couple of years.

Corporate virtual PPAs are available under a ‘sandbox’ initiative launched by the electricity sector regulator in 2019. The first corporate virtual PPA under this sandbox initiative was announced in February 2025 and is expected to serve as a benchmark for future development of this contractual structure in Thailand.

Renewable energy incentives

The ERC has established two incentive schemes to assist data centre operators with sourcing renewable energy. These initiatives respond to growing international demand for data centres to operate solely on clean energy sources:

- The **Utility Green Tariffs (UGT) program**, which is split into two phases as follows:
 - UGT1 enabled data centre operators to purchase renewable electricity – including solar, wind, hydro and biomass – certified by I-REC Renewable Energy Certificates. Applications for UGT1 closed on 28 February 2025.
 - UGT2, expected to be launched by mid-2025, will enable users to purchase electricity from specific portfolios of renewable energy projects.
- The **DPPA scheme**, allowing data centre operators to directly procure up to 2,000MW of renewable energy from producers. Expected to launch in the second half of 2025, the scheme will initially target users requiring 50MW or more, with smaller users (from 5MW) phased in gradually. These Direct PPAs will include clear terms for transmission line usage fees and energy generation locations.

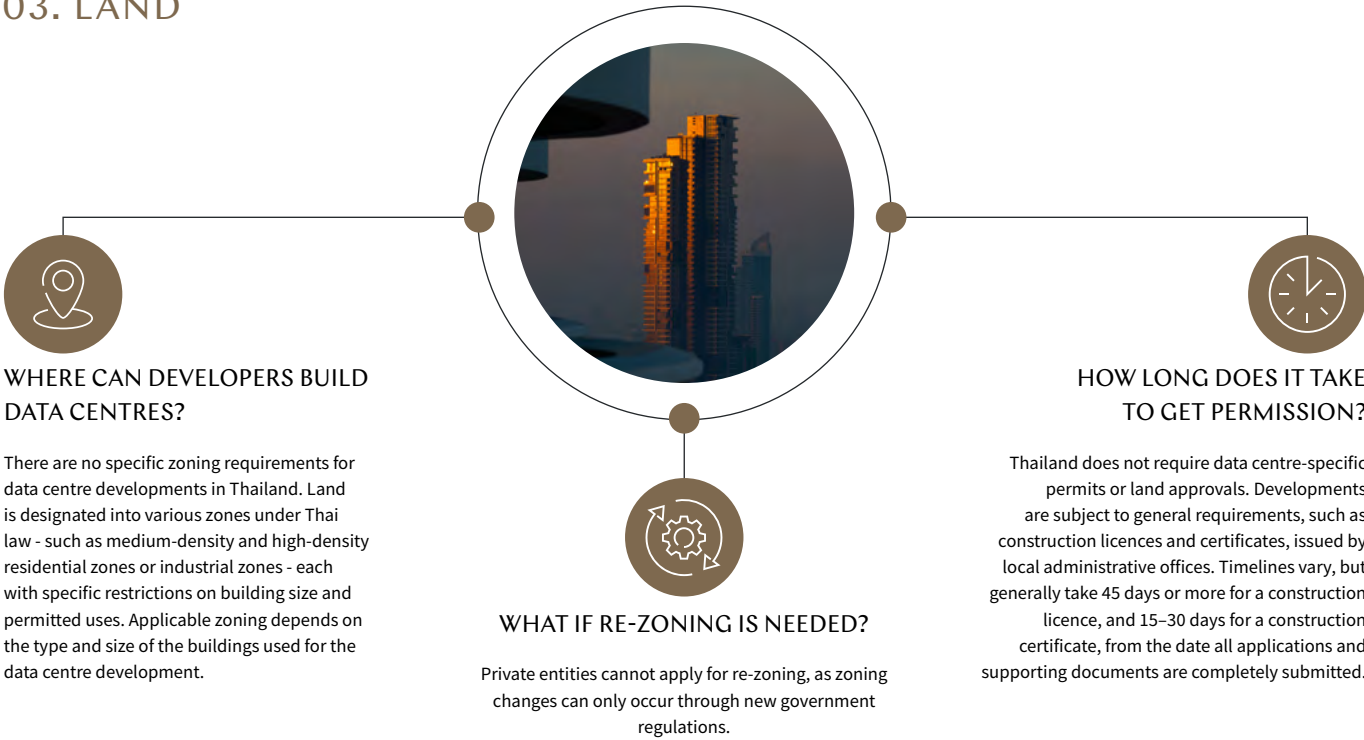


02. WATER

Water supply

Water supply in Thailand is generally reliable. Responsibility for water supply rests with the Metropolitan Waterworks Authority (**MWA**) in the Bangkok metropolitan area, and the Provincial Waterworks Authority (**PWA**) for the rest of the country. While water shortages can occur during periods of drought, particularly in rural areas, major urban centres (where data centres are typically located) have stable and secure water supplies.

03. LAND



04. TELECOMMUNICATIONS

Are data centre operators required to obtain a telecommunications licence?

Under the *Telecommunications Business Operations Act B.E. 2544 (2001)* (**TBOA**), data centres are classified as **regulated telecommunications businesses**, even if they do not provide network services. Under the TBOA, a data centre operator is required to obtain a Type-1 Telecommunication Operating Licence (**TOL**). A Type 1 TOL, defined as 'telecommunications without its own physical network and provided freely', is available to foreign-majority owned companies. In comparison to other licence types, a Type 1 TOL has no foreign ownership restrictions (however, see Section 5, Foreign Investment Restrictions, below).

The scope of permitted activities is determined on a case-by-case basis, and applicants must submit a complete business plan to the National Broadcasting and Telecommunications Commission (NBTC) to ensure the licence fully covers their intended operations. However, one of the key restrictions under a Type 1 TOL is that the operator cannot control or operate a telecommunications network.



STRATEGIC OPPORTUNITIES

05. FOREIGN INVESTMENT RESTRICTIONS

Land

Foreign individuals, foreign-incorporated entities, and Thai companies with over 49% foreign ownership or majority foreign shareholders are **generally prohibited from owning land** in Thailand, subject to limited exceptions.

One common exception allows eligible foreign businesses to own land through incentives granted by the BOI. For data centres, BOI incentives include an 8 year corporate income tax exemption and land ownership rights (see [Section 6](#) Tax and other incentives below).

Data centres

Under the *Foreign Business Operator Act B.E. 2542 (1999)* (**FBOA**), foreign entities are prohibited and restricted from developing or owning a data centre unless they obtain:

- a foreign business license (**FBL**), which is granted on a case-by-case basis. The application procedure involves submitting a detailed business plan, including 3 year estimated revenues and expenses, for approval by the Foreign Business Operation Committee, which consists of high-ranking officers from various governmental authorities. The entire process may take approximately 4–6 months, or longer in unusual cases.
- a foreign business certificate (**FBC**), which is only applicable if foreign entities are granted permission to operate a restricted business under the *Investment Promotion Act, B.E. 2520 (1977)*, the *Industrial Estate Authority of Thailand Act, B.E. 2522 (1979)*, or treaties to which Thailand is a party.

Unlike an FBL, obtaining an FBC is straightforward, and the process typically takes approximately 2 weeks, though it could take up to 30 days in unusual cases. Therefore, if feasible, an FBC is preferable to an FBL.

A Thai-incorporated company is deemed foreign under the FBOA if 50% or more of its share capital is held by:

- foreign individuals
- foreign juristic entities, or
- Thai juristic entities in which 50% or more of the share capital is held by:
 - foreign individuals;
 - foreign juristic entities; or
 - Thai juristic entities in which 50% or more of the share capital is held by foreign individuals or juristic entities.

In assessing foreign ownership, the analysis must be conducted on a tier-by-tier basis up the corporate ownership chain, typically up to the ultimate parent company.

06. TAX AND OTHER INCENTIVES

Special economic zones and corridors

Thailand has established several SEZs and economic corridors with incentives offering both tax and non-tax benefits to attract investment. These areas offer favourable conditions to support the establishment and operation of data centre developments, and include:

- over 15 SEZs including 10 along its borders to enhance trade with neighbouring countries, and
- 4 new economic corridors in the north, north-east, central-west and the south.

THE EASTERN ECONOMIC CORRIDOR IS A PARTICULAR FOCUS, EARMARKED AS THAILAND'S 'SILICON VALLEY' FOR TECHNOLOGY AND INNOVATION.

Tax incentives

The BOI may grant up to 8 years of corporate income tax exemptions for data hosting service providers that:

- lease host servers for data storage
- operate at least 2 data centres in Thailand that meet or exceed the ISO/IEC 27001 data centre standard
- invest a minimum of THB 5 billion, and
- maintain a debt-to-equity ratio no greater than 3:1.

Additional incentives include:

- VAT exemptions for VAT-registered Thai-incorporated operators
- exemption on duties and taxes for imported machinery
- the right for foreign investors to obtain a FBC, bypassing standard licensing procedures
- land ownership rights for the promoted business, and
- a special allotment of work permits to employ foreign professionals with more relaxed requirements.

Other incentives

In addition to BOI incentives, Thailand has established agencies like the Digital Economy Promotion Agency and National Science and National Innovation Agency which offer funding and general government support.



COMPLIANCE AND RISK MANAGEMENT

07. DATA PROTECTION AND CYBER SECURITY

Data protection and privacy framework

Thailand does not have laws specifically targeting data centre operators, developers and customers. Instead, data centres are subject to the *Personal Data Protection Act B.E. 2562 (2019) (PDPA)*, which applies across all industries. Depending on their services and contractual arrangements, **data centres may be classified as data processors** or, in some cases, **data controllers**, and must comply with relevant PDPA obligations, particularly around data security.

This includes implementing technical and organisational measures to protect personal data against loss, unauthorised access, or unlawful processing, such as physical safeguards, access controls, encryption and audit capabilities.

Data centres must also assist data controllers in meeting obligations regarding data subject rights and breach notifications.

Sector-specific regulators such as the Bank of Thailand, the Securities and Exchange Commission, and the NBTC may impose additional requirements to the PDPA for regulated entities.

Cyber security laws

Cyber security is primarily governed by the PDPA and the *Computer-Related Crime Act B.E. 2550 (2007) (CCA)*. The CCA criminalises unauthorised access, data interception, and unlawful alteration or destruction of data or systems, including those operated by data centres.

Data centre operators are required to implement strong physical and cyber security measures to ensure compliance. Operators providing hosting or cloud services may also qualify as service providers under the CCA, requiring them to retain traffic data and cooperate with lawful requests from authorities.

In addition, data centre operators designated as critical information infrastructure (**CII**) (see [Section 8](#) Critical infrastructure and security below) may be subject to notifications issued by the National Cyber Security Committee (**NCSC**) or Cyber security Regulating Committee which impose cyber security standards, codes of practice and operational guidelines.

Operational resilience obligations

Thailand does not have specific laws or regulations on operational resilience for data centres. However, operators typically follow the Uptime Institute's internationally recognised data centre classification standards.

08. CRITICAL INFRASTRUCTURE AND SECURITY

Under the *Cybersecurity Act B.E.2562 (2019) (CSA)*, computer and IT systems which are critical to national security, military security, economic security, and public order are regulated as CII. Data centres may be considered CII if they are used to provide services relating to national security, military security, economic security, and public order.

If a data centre is considered CII, the CSA requires the data centre operator to:

- implement both cyber security and physical security measures to prevent, mitigate, and respond to cyber threats
- conduct risk assessments, incident response planning, and access controls to protect data and systems, and
- adopt a proactive security posture, including measures to prevent unauthorised physical access that could compromise the integrity or availability of critical systems and data hosted in the data centres.

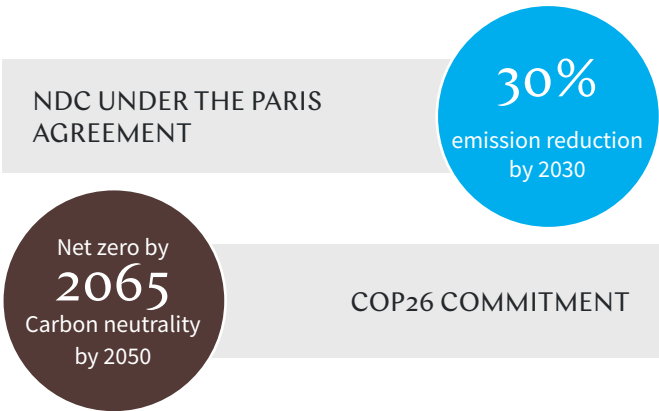
09. DATA LOCALISATION

Thailand does not impose data localisation or residency requirements, even for sensitive data or specific sectors.

10. ENVIRONMENTAL, SOCIAL AND GOVERNANCE

International ESG commitments

Thailand is a signatory to the UN Framework Convention on Climate Change, the Kyoto Protocol, and the Paris Agreement. While there is currently no federal law implementing these commitments, a draft Climate Change Bill - led by the Department of Climate Change and Environment and the Ministry of Natural Resources and Environment - is expected to be enacted in 2026.



ESG reporting

Generally, ESG reporting is not mandatory in Thailand. However, **listed companies** are required to report annually via Securities and Exchange Commission Form 56-1 (**Form 56-1**). Under the Form 56-1 Reporting Guide, there are reporting guidelines in respect to a company's:

- high-level policies and practice guidelines regarding environmental matters, and
- performance in environmental management, particularly in areas significant to its business operations, such as energy consumption management.

Listed companies are also required to report their GHG emissions in accordance with international standards or an equivalent framework. These disclosure requirements follow a 'comply-or-explain' basis – companies that do not report must explain why. Unlisted companies are not subject to these requirements.

11. SECTOR-SPECIFIC REGULATIONS APPLICABLE TO DATA CENTRES

Government bodies

The NCSC has published the **NCSC Notification Re: Cloud Cyber security Standards** which applies to governmental bodies and CII organisations. The notification sets out requirements to adhere to prescribed cloud cyber security standards under two areas: cloud security governance and cloud infrastructure and operations.

A regulated entity must comply with the requirements under these standards to varying degrees, depending on the level of impact that its data or information systems have on its operations.

THE IMPLEMENTATION OF THESE STANDARDS MUST BE REPORTED TO THE NATIONAL CYBER SECURITY AGENCY.

Financial services providers or financial institutions

The Bank of Thailand has published the **Notification Re: Regulations on IT Sourcing for Business Operations of Financial Institutions** (No. FPG 19/2559) which applies to financial institutions that engage third parties for IT services (including cloud computing). Under this notification, engagement of third-party IT outsourcing (for example, data centre operators) by Thai financial institutions will require approval from the Bank of Thailand.

Those IT outsourcing services must comply with various control requirements depending on the criticality of the service. For example, the notification sets out policies on outsourcing, risk management, service provider management, and security, integrity and availability of IT systems and information.



VIETNAM

CHAPTER 13

SNAPSHOT



Vietnam is growing as a data centre market from a relatively low base. There is strong government support for data centre investment. Recent legislative changes provide greater certainty around foreign ownership, PPAs and the regulatory status of data centres, while strategic incentives and benefits are available including at special high-tech parks.

With a growing and digitally savvy population, Vietnam is focused on digital transformation and infrastructure development. Foreign capital is needed to supplement the domestic response to the increasing demand for data centre services. This is promising, provided that existing power stability issues can be overcome to sustain growth.

OPPORTUNITIES

- ✓ No foreign investment limits
- ✓ High-tech parks and various incentives
- ✓ New green power purchasing framework (direct PPAs)

CHALLENGES

- ✗ Environmental requirements particularly for water use
- ✗ Power stability issues

SPOTLIGHT ON KEY DRIVERS

THERE'S NO LIMIT

The **Law on Telecommunications 2023 (Telecoms Law)** confirmed that there is no limit on foreign ownership of companies providing data centre services or cloud services in Vietnam.

While this is **not officially a change in law** as there was no specific limit previously, this is the first time that it has been confirmed in law. The **regulatory clarity** will provide foreign investors with more confidence to invest in the Vietnamese data centre industry.

THE RIGHT INCENTIVES

Vietnam has several high-tech parks and SEZs in central and strategic locations.

These offer favourable conditions and incentives for data centre investments, including:

- **supporting infrastructure** well-suited to data centre operations such as access to power and telecommunications networks, and
- **tax breaks and other incentives** including corporate income tax incentives, import duty exemptions and land and water surface rent exemptions.

AN EVOLVING REGULATORY LANDSCAPE FOR DATA

New obligations dramatically heighten the burden for companies handling data.

On the back of data localisation, security and privacy reforms in recent years, the **Law on Data 2024 (Data Law)** came into effect on 1 July 2025. In parallel, a decree giving the implementation of the Data Law (**Data Decree**) was issued on 30 June 2025 and came into effect on 1 July 2025.

The Data Law and Data Decree:

- heighten obligations for handling important data, including by foreign-owned enterprises, to address national security concerns
- restrict the transfer of important data outside of Vietnam (see Section 9 Data Localisation below)
- restrict the transfer of important data outside of Vietnam, and its use by Vietnamese and foreign entities, and
- introduce licensing or registration for certain data-related products and services, which may include data centre and data processing services.

What are the legal instruments in Vietnam?

Each of these legal instruments is generally subordinate in priority to the instruments issued by higher authorities. They may vary in detail - from high-level principle documents to more technical and granular instruments.

INSTRUMENT	OVERVIEW
LAWS	Drafted by a government Ministries and approved by the National Assembly, the highest legal authority.
DECREES	Issued by Ministries without Assembly approval, detailing how laws are implemented.
CIRCULARS AND DECISIONS	Issued by Ministry heads or equivalent authorities, explain how laws or decrees are applied. Decisions may also come from Local People's Committees (executive body of a province).
RESOLUTIONS	Similar in function to circulars and decisions and issued by Local People's Councils (legislative body of a province).

'Vietnam's increasingly mature legal framework on telecommunications, data and cyber security has removed previous legal uncertainty, enabling a more open, investor-friendly regulatory environment that supports sector growth and simplifies compliance for foreign providers.'

Ho Thuy Ngoc Tram
Partner
Frasers Law Company



OPERATIONAL

01. POWER

Getting power to a site

The State-owned power company, EVN, has an effective (but not statutory) monopoly over mains power supply in Vietnam. Non-State entities can be granted a right to invest in and construct transmission grids, but none have to date.

Vietnam’s electricity market is undergoing phased liberalisation, allowing non-State entities to participate in power generation and distribution activities, though the regulatory oversight is stringent.

There is a **multi-step process to secure power** to a site from EVN and its local brands. Timelines vary based on location and entity type, though typically range from **3 months to over a year**, with shorter timelines for urban areas close to existing power infrastructure versus rural and remote sites with limited connectivity.

Recent government efforts have accelerated some processes, particularly in industrial zones, with new transmission lines typically completed in 6 months or less rather than 12 months or more as may have been the case historically. In some provinces, EVN may expect data centre developers to invest in grid infrastructure or private substations.

Power purchase agreements

Specific government circulars apply to PPAs depending on the project.

- **Small-scale hydropower projects**
Use avoided cost tariffs, which involve rates based on the costs that the power utility does not need to incur thanks to the power generated by the project.
Circular 10/2025/TT-BCT (1 February 2025)
- **Thermal power** (coal, gas, LNG) and **renewable energy** (saves for certain limitations)
Circular 12/2025/TT-BCT (1 February 2025)
- **New wind and solar projects**
Apply to those participating in the Vietnam Wholesale Electricity Market and large scale (≥30MW) and mini hydropower projects.
Circular 12/2025/TT-BCT (1 February 2025).

Since Decree 80/2024/ND-CP in July 2024 (**Decree 80**), which has now been replaced by Decree 57/2025/ND-CP dated 3 March 2025 (**Decree 57**) with clearer regulatory pathways, large electricity consumers can enter into direct PPAs (**DPPAs**) with renewable energy generators under two mechanisms – the National Power Grid Model and the Private Line Model.

- **National Power Grid Model (or virtual DPPA)** involves executing a DPPA and delivering electricity through the national grid between the renewable power generator and large electricity consumers (or authorised electricity retailers within industrial zones or clusters), and comprises the following arrangements:
 - the renewable power generator enters into an agreement with EVN to sell its entire power output into the national grid, with all generated electricity traded on the spot market of the competitive wholesale electricity market
 - the large electricity consumer (or authorised electricity retailer in industrial zones or clusters) enters into a forward electricity contract—structured as a financial contract-for-difference - with the renewable power generator, effectively fixing the price between the two parties, or
 - the large electricity consumer (or authorised electricity retailer in industrial zones or clusters) also enters into a PPA with the power corporation (or its authorised or delegated units) to procure all electricity required for its actual consumption from the grid.
- **Private Line Model (or physical DPPA)** facilitates electricity trading through term contracts between renewable energy generators and large electricity consumers (or authorised retail electricity units in designated zones or clusters) via power lines built directly from generator to consumer site. This suits businesses near renewable energy sites with the capacity to support a dedicated line, meaning there is no need to rely on the national grid.

Decree 57 prescribes certain mandatory terms for each of the contracts involved in these DPPA models, as well as licensing requirements and eligibility criteria for participants in either model.

Going ‘green’

Vietnam’s government is actively promoting ‘green’ data centres to reduce energy consumption and carbon emissions through its legal framework and continuing commitments to sustainability through a number of initiatives.

• Approvals stage requirements

Data centre projects to undertake environmental impact assessments (**EIAs**) and submit them for appraisal by a council of experts. These experts are appointed by a relevant government appraising authority – typically the Ministry of Natural Resources and Environment or Provincial People’s Committee depending on the nature of the project.

If the appraisal approves the project, then the relevant authority may issue investment approvals (see [Section 3](#) Land below). The project operator must comply with the conditions of the EIA.

• Energy efficiency and stability in operations

Under the Information and Communication Infrastructure Master Plan for the Period 2021–2030, with a Vision to 2050, approved by Decision No. 36/QĐ-TTg in January 2024 (**Decision 36**), the development orientation is to establish large-scale data centres built to green standards and aligned with regional energy planning. Accordingly, new data centres are required to meet international green benchmarks, including achieving a PUE of 1.4 or lower.

Priority is given to locations with stable electricity supply, supported by at least two independent medium-voltage substations. Decision 36 also encourages the selection of sites in close proximity to renewable energy sources.

Decision No. 1132/QĐ-TTg, issued by the Prime Minister on 9 October 2024, approved the Digital Infrastructure Strategy to 2025 with an orientation to 2030 and sets out the following vision:

DIGITAL INFRASTRUCTURE IS THE FOUNDATION FOR VIETNAM TO BECOME A MODERN AND SMART DIGITAL NATION. IT WILL BE ADVANCED, MODERN, WELL-COORDINATED, SECURE, AND SUSTAINABLE, ON PAR WITH DEVELOPED COUNTRIES, THEREBY HELPING VIETNAM ACHIEVE UPPER-MIDDLE-INCOME STATUS BY 2030 AND HIGH-INCOME STATUS BY 2045.



02. WATER

Water supply

As Vietnam continues to urbanise and industrialise, competition for water use among the agriculture, manufacturing and residential sectors has intensified. Certain regions of Vietnam are prone to rain shortages and seasonal droughts. Particularly in those regions, authorities are giving increased weight to water use efficiency in environmental permitting. In practice, data centres are expected to incorporate closed-loop cooling, water cycling and other conservation technologies.

Environmental advocacy in Vietnam is also driving stricter oversight of industries with high water consumption, including data centres.

Increasing focus on efficiency

The Vietnam government has strengthened environmental regulations and imposed water efficiency requirements and recommendations through the introduction of the following laws and regulations.

Key laws and regulations

LAW ON ENVIRONMENTAL PROTECTION 2020

EIA approvals and environmental permits will not be issued for new investment projects that discharge wastewater directly into overloaded surface water bodies, unless such projects incorporate measures to treat the wastewater to environmental standards, reuse it, or assist in restoring polluted areas.

Project owners are also required to submit annual (or ad hoc) environmental protection reports, detailing the performance of environmental protection facilities and waste management measures.

LAW ON WATER RESOURCES 2023

Water must be used economically and efficiently, with a prohibition on the discharge of wastewater into surface water bodies unless environmental technical standards are met.

Depending on the volume of use, project owners must declare, register and obtain a licence for the exploitation and use of water resources.

CIRCULAR NO. 02/2014/TT-BCT

Industrial sectors, including data centres, must conduct water usage audits and adopt measures for hot water supply systems as part of broader energy efficiency and conservation obligations.

QCVN 08:2023/BTNMT (SURFACE WATER QUALITY STANDARDS)

Surface water is classified into four quality levels — A (good), B (moderate), C (poor), and D (very poor) — to guide usage and safeguard aquatic ecosystems:

- Level A: Suitable for domestic use, swimming, and recreation (after treatment)
- Level B: Suitable for industrial and agricultural use (after treatment)
- Level C: Odour-free and suitable for industrial use (after treatment), and
- Level D: Limited to water transport and other low-quality uses.

Compliance with wastewater discharge standards and efficient water use policies are key factors in data centre site selection and operational planning.

03. LAND

No land ownership

Land is considered public property in Vietnam and is owned by the State. Although individuals and entities cannot privately own land, they can seek leases to unlock opportunities, including foreign investors.

Land use rights

Foreign-owned entities can obtain land use rights either from the State, an existing land user or by forming a joint venture with a local entity.

How to obtain land use rights as a foreign investor



FROM THE STATE
Leasing land



- IN INDUSTRIAL OR HIGH-TECH ZONES
- Sub-leasing land within the relevant zone
 - Acquiring land use rights from an existing land user



- WITH A LOCAL PARTNER
- Joint venture
 - Local partner contributes land use rights as capital

Leasing land from the State can take several months, as it requires compliance with several administrative procedures and may involve a bidding process.

- **A competitive bidding process** is required where there are multiple interested parties or there is a large-scale project.
- **Commercial negotiations** are possible where there is no competitive bidding process required, involving foreign investors dealing directly with landholders for rights. This may be less administratively complex, but timelines will depend on the progress of the commercial negotiations and relative bargaining power of the parties.

Investment approvals

Before commencing a foreign-invested data centre project in Vietnam, the project must typically secure an Investment Policy Approval (**IPA**) and an Investment Registration Certificate (**IRC**).

An IPA is generally required where capital or land requirements for the project meets thresholds under the *Law on Investment 2020 (Investment Law)*.

The municipal People’s Committee, or a special zone management board, will review IPA requests for most data centre projects, except for projects involving facility-based telecommunication services which require approval from the Prime Minister. The relevant State investment authority will issue an IRC within 5 to 15 working days of the IPA. In total, the IPA and IRC processes typically take 90 days or more from submission.

Construction permit

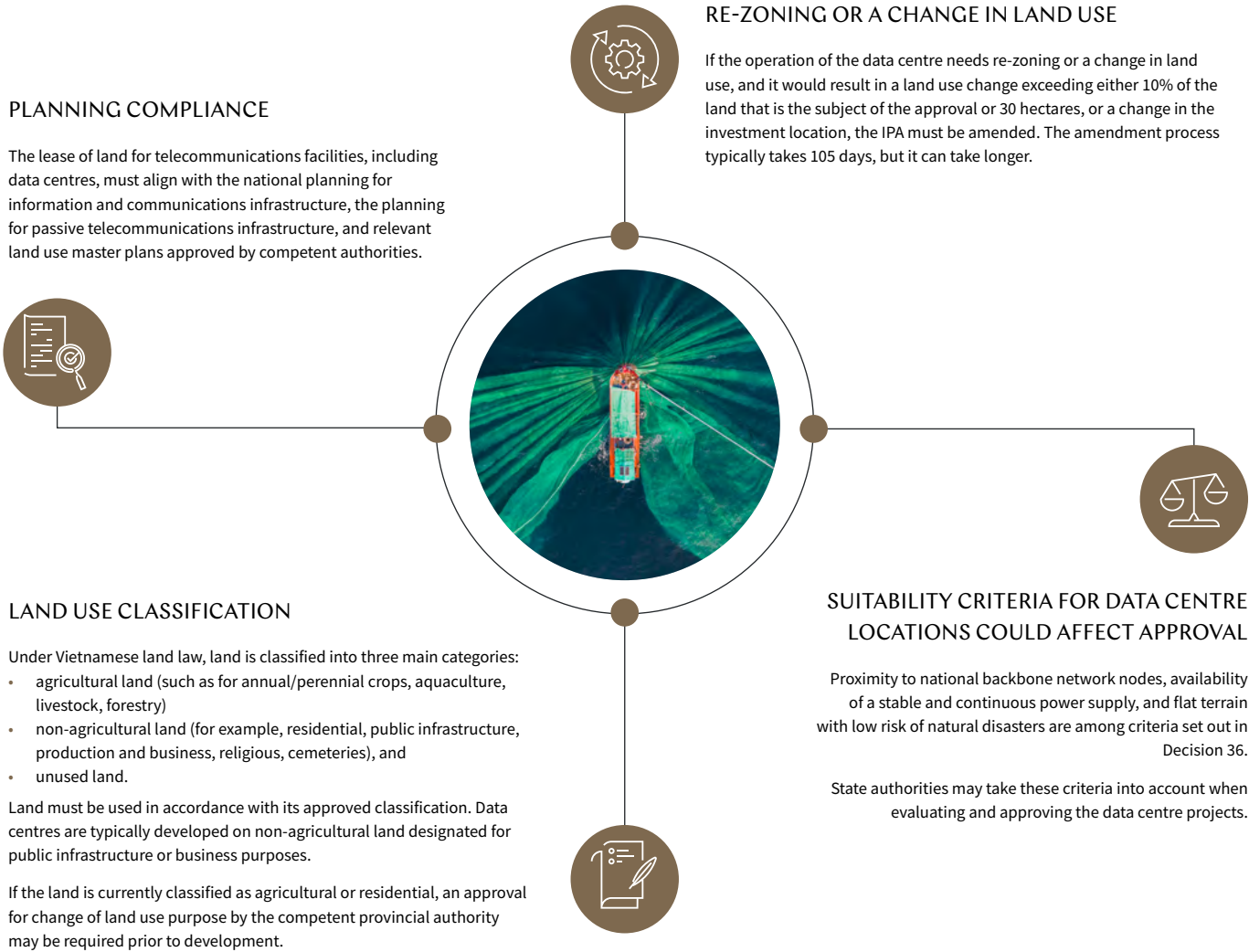
In addition to obtaining an IPA and IRC for a data centre project, a construction permit will be required before commencing construction of a building or facility on the relevant site. Construction permits are mostly issued by the Provincial People’s Committee in the relevant province.



What are the zoning requirements?

The zoning requirements for data centres are generally the same as for standard investment projects, with the exception that data centre projects which involve facility-based telecommunications services require an IPA from the Prime Minister.

Currently, there are **no legal restrictions on the land or geographical areas** where data centres may be constructed. However, similar to other land-based investment projects, data centre developments must comply with applicable land use master plans and planning instruments.



04. TELECOMMUNICATIONS

Is a telecommunications licence required?

Whether a licence is required depends on the services provided at and to the data centre. There are two arrangements:

- **No licence is needed** for a pure ‘data centre service’ (in other words, services providing functions including processing, storage and extraction of information for users via the telecommunications network by leasing part or all of the data centre), other than the registration requirement outlined below
- **Individual licences** may be needed if the data centre operator traditional telecommunications services along with the data centre service (for example, internet access services used to connect between physical data centre sites) -the licences required would depend on whether the data centre operator owns the underlying network infrastructure used for the telecommunications services or not.

Applicability of telecommunications laws to data centres

The Telecoms Law, and Circular No. 03/2013/TT-BTTTT as amended by Circular No. 23/2022/TT-BTTTT of the Ministry of Information and Communication dated 13 February 2023 (**Circular 03**), provide a light-touch regulatory framework for data centre services, over-the-top services and cloud computing services.

Framework obligations for data centre operators:

- register with the Minister of Information and Communications (**MOIC**) to obtain a certificate of registration for the provision of telecommunications services prior to offering data centre services
- one of the conditions is the submission of a technical plan that aligns with information and communications infrastructure planning, complies with applicable standards and technical regulations, and ensures the safety of telecommunications infrastructure, cyber security and information security
- obtain a telecommunications service registration certificate, or notify the MOIC to provide data centre services on a cross-border basis
- notify the Vietnam Telecommunications Authority in a specified form of the services the data centre operator will be providing
- store certain identification information of its customers
- refrain from accessing customer data or tracking customer communications without consent of the customer, and
- prevent access to certain information, where directed by State authorities.



STRATEGIC OPPORTUNITIES

05. FOREIGN INVESTMENT RESTRICTIONS

Land

While land cannot be privately owned, there are no foreign investment restrictions in relation to land use rights (see [Section 3](#) Land above).

Data centres

There are no foreign ownership limits for enterprises providing data centre services, meaning foreign investors may own up to 100% equity.

Telecommunications service providers

There are no restrictions on foreign ownership of non-facilities-based telecommunication services. However, there are foreign ownership caps for telecommunication service providers who:

- invest in telecommunications infrastructure and own transmission capacity – up to 50%, and
- do not own infrastructure or transmission capacity but contract with a facilities-based provider – up to 65%.

These restrictions are relevant where a data centre operator is also providing traditional telecommunications services bundled with the data centre services, for example, as part of an internet exchange business (see [Section 4](#) Telecommunications above).

06. TAX AND OTHER INCENTIVES

Special economic zones

Several high-tech parks and economic zones offer favourable conditions and incentives for data centre investments. Key SEZ locations for data centre investments include:

SAIGON HI-TECH PARK

Located in Ho Chi Minh City, offers land leases, tax breaks and support services

DA NANG HI-TECH PARK

Located in Da Nang, a central location in Vietnam

HOA LAC HI-TECH PARK

Located in Hanoi, focusing on IT, biotech and new materials attracting high-tech investments

Financial incentives for high tech industries

The Investment Support Fund (**ISF**), established in 2024 under Decree No. 182/2024/ND-CP, is designed to provide financial incentives for high-tech enterprises, including high-tech data centre developments and operations.

The ISF offers two support models for eligible projects (which are not mutually exclusive).

- Annual expense support** provides eligible data centre projects access to financial assistance for operational expenses such as training and human resource development, research and development (**R&D**), and high-tech product manufacturing.
- Initial investment cost support** covers up to 50% of initial investment costs for establishing R&D centres in sectors such as AI, subject to specific conditions. To qualify for these incentives, data centre projects must have either:
 - a minimum capital of VND6,000 billion (approximately US\$260 million)
 - an annual revenue of at least VND10,000 billion (approximately US\$430 million), or
 - committed capital to be disbursed within a specified period, typically VND12,000 billion (approximately US\$460 million) within 5 years from the IRC issuance or equivalent legal document. For certain specific industry projects such as AI data centres, the committed capital requirement is reduced to VND6,000 billion within 5 years or VND4,000 billion (approximately US\$153 million) within 3 years from the issuance of the IRC or equivalent legal document.

Tax and other incentives

Investment projects in industrial zones and high-tech parks may qualify for incentives depending on location and the nature of the project.

Common incentives include preferential tax rates, tax holidays, import duty exemptions (including for capital goods such as machinery, equipment and specialised vehicles used to form fixed assets, and raw materials), and land and water surface rent exemptions.

COMPLIANCE AND RISK MANAGEMENT

07. DATA PROTECTION AND CYBER SECURITY

A modernising data protection framework

Vietnam’s modernising data protection framework mostly impacts the customers of data centre operators. However, there are considerations for data centre operators – particularly in relation to ensuring that the Ministry of Public Security (**MOPS**) can continue to exercise its inspection powers in respect of personal data.

The data protection framework includes several key data localisation requirements (see [Section 9](#) Data localisation). In particular:

- the **Data Law restricts the transfer of critical information** outside of Vietnam
- Decree No. 13/2023/ND-CP (**Decree 13**) regulates personal data and prohibits the processing of Vietnamese personal data **without the fully informed consent** of the data subject, except in certain cases such as to protect a person’s life or health or to fulfil the data subject’s contractual obligations, and
- Decree 13 also requires persons transferring Vietnamese personal data outside of Vietnam to **prepare an impact assessment** to be filed with the MOPS, and ensure that the relevant personal data is available for the Ministry’s inspection.

THE PERSONAL DATA PROTECTION LAW (PDPL) WAS PASSED IN LATE JUNE 2025. THE PDPL LARGELY REPRODUCES AND EXPANDS UPON THE OBLIGATIONS UNDER DECREE 13, ADDING ADDITIONAL CONSENT REQUIREMENTS FOR CERTAIN TYPES OF DATA OR PROCESSING AND AN OPT-IN/OPT-OUT REGIME FOR THE USE OF PERSONAL DATA FOR TARGETED ADVERTISING. IT IS CURRENTLY EXPECTED THAT THE PDPL WILL TAKE EFFECT FROM 1 JANUARY 2026.

Cyber security laws focused on national security

Vietnam’s cyber security laws include obligations traditionally present in other regimes, such as obligations to:

- secure data and networks; and to report cyber security incidents to relevant local police authorities, or Bureau of Cybersecurity, and
- High-Tech Crime Prevention and Control (A05) within the MOPS (depending on where the relevant data controller is located).

However, the main focus of Vietnam’s cyber security laws is national security.

The *Law on Cybersecurity 2018* (**Cybersecurity Law**) and the associated guidance Decree No. 53/2022/ND-CP (**Decree 53**) require:

- data centre operators (when managing and operating national cyberspace infrastructure and networks, and potentially providing telecommunications services) to implement **cyber security technical measures** and comply with government cyber security directives
- data centre operators and their customers to comply with requests from the MOPS to store, and provide access to, data for cyber security investigations and national security purposes, and
- service providers that perform data collection or processing activities using personal data of Vietnamese users or telecommunications service providers where directed by the government to comply with certain **data localisation obligations** (see [Section 9](#) Data localisation).

What are the localisation requirements?

The Cybersecurity Law requires providers of telecommunications, internet, cloud computing or data storage services (including data centre operators) to store certain personal data, user activity logs and other information within Vietnam (**Localisation Requirement**) (see [Section 9](#) Data localisation).

The Localisation Requirement was enhanced by the Telecoms Law and Decree No. 163/2024/ND-CP (**Decree 163**), which extend the Localisation Requirement to foreign providers of cloud computing and data centre services when operating in Vietnam, and the Data Law will further enhance this.

As a corollary to this data-sharing requirement, data centre operators must assist in cyber security investigations and national security matters under Decree 13 and comply with storage and access requests from MOPS as noted above.



08. CRITICAL INFRASTRUCTURE AND SECURITY

Critical infrastructure laws

Data centres are not explicitly characterised as ‘critical infrastructure’. However, they are subject to stringent regulatory oversight by the MOPS under the Cybersecurity Law (see [Section 7](#) Data protection and cyber security). Further, data centre operators must:

- **register with or notify the MOIC** prior to offering services in Vietnam (see [Section 4](#) Telecommunications), and
- meet requirements relating to **data security, service quality, and state cooperation**.

A focus on national security

There is a thread of national security through the laws of Vietnam.

- The Cybersecurity Law and Decree 13 impose national security obligations on data centre operators (see [Section 7](#) Data protection and cyber security).
- The Telecoms Law also imposes national security obligations, with government oversight, as it regulates telecommunications infrastructure, including data centres, with a view to safeguarding national security and public order.

For example, any organisation that **detects acts of sabotage or interference** with telecommunications infrastructure must notify the local police authorities and People’s Committees. Data centre operators who own infrastructure used in telecommunications networks must protect that infrastructure and ensure they do not cause damage to or adversely affect telecommunications infrastructure owned by others.



Physical security standards

National Standard TCVN 9250:2021 requires data centres to have access control systems to prevent unauthorised entry, with continuous surveillance using CCTV. The MOIC may also specify technical standards that data centres must comply with before operations commence.

Technical standards or accreditations

Data centres in Vietnam must comply with specific domestic standards to meet technical, safety and operational requirements, which are established under several regulations including the Telecoms Law and Circular 03.

Compliance with these regulations is mandatory before operations can commence.

- Data centre operators are entitled to engage in **R&D and pilot implementation** of new technologies and models in telecommunications, as well as being responsible for compliance with mandatory network and service management requirements, in accordance with the Telecoms Law.
- Data centre operators must assess and publicly disclose their compliance with prescribed **standards and technical assurance levels** (in addition to the physical security standards contained in the National Standard TCVN 9250:2021, above).

This includes the National Technical Regulation on Lightning Protection (QCVN 32:2020/BTTTT), National Technical Regulation on Grounding (QCVN 9:2016/BTTTT) and the National Technical Regulation on Fire Safety (QCVN 06:2021/BXD).

09. DATA LOCALISATION

Localisation requirement

Despite appearing broad in nature, the Localisation Requirement (see [Section 7](#) Data protection and cyber security) does not impose a general data localisation or residency requirement on all types of data. It requires Vietnamese enterprises to **store certain types of Vietnamese user data** within Vietnam, including:

- personal data
- user-generated data, such as like account names, service usage time, credit card details, email and IP addresses, and registered phone numbers, and
- relationship data, such as like users’ contacts, groups and networks.

Copies of that data may be transferred abroad if applicable legal requirements are complied with.

According to the Data Law, the **cross-border transfer of core and important data** must comply with principles of national defence and security, national and public interest, and the protection of the lawful rights and interests of data subjects and data owners. This much be done in accordance with Vietnamese law and international treaties to which the Socialist Republic of Vietnam is a party.

A key principle set out in the Data Decree (Decree No.165/2025/ND-CP) is the clarification of the meaning, and conditions and cross-border transfer and processing, of core and important data.

The Data Decision (Decision No. 20/2025/QĐ-TTg on important and core data classification) was issued and came into effect on 1 July 2025. It provides an indicative list of important and core data. While most of these categories pertain to State-related activities, certain private-sector data types are also covered.

DATA TYPE	DESCRIPTION	EXAMPLES	TRANSFER CONDITIONS
IMPORTANT DATA	Data that could potentially impact national defence, security, foreign affairs, macroeconomic stability, social order, public health or community safety	<ul style="list-style-type: none">• Confidential banking data, account information, and loan data involving 10,000 or more Vietnamese businesses or organisations, and• Basic personal data of 100,000 or more individuals.	<p>At least 15 days before transferring or processing important data across borders, data administrators must prepare and submit a Cross-Border Data Transfer and Processing Impact Assessment Report (Impact Assessment Dossier) to the Ministry of National Defence (for military, defence, or cryptographic data) or to the MOPS (for other fields) (together, the Data Regulators).</p> <p>Data administrators may proceed with the cross-border data transfer or processing without prior approval from the Data Regulators.</p>
CORE DATA	Data that directly affects the above areas	<ul style="list-style-type: none">• Confidential banking data, account information, and loan data involving 100,000 or more Vietnamese businesses or organisations• Basic personal data of 1,000,000 or more individuals, and• Sensitive personal data of 100,000 or more individuals.	<p>As with important data, data administrators must submit an Impact Assessment Dossier to the Data Regulators, except in limited cases.</p> <p>The Data Regulators must complete its review within 10 working days from receipt of a complete and valid dossier. The transfer or processing may only proceed upon receipt of a positive assessment from the relevant authority.</p>



Application to foreign entities

The Localisation Requirement mainly impacts local entities.

However, a foreign entity providing telecommunications networks, internet services or value-added services (such as data centre services or cloud services) in Vietnam and engaging in user data collection, exploitation, analysis or processing **may be required to store data**, and **establish a branch or representative office**, locally if:

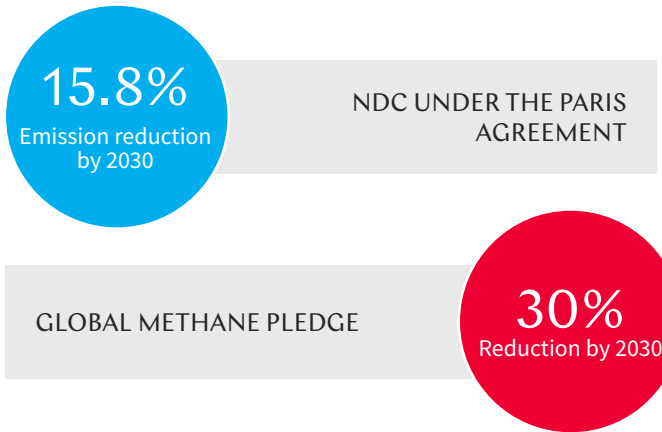
- its services are used in **violations** of the Cyber security Law
- it receives a **violation notice** from the MOPS requiring cooperation in prevention, investigation or enforcement, and
- it **fails to comply**, or only partially complies, with directions of relevant authorities, or obstructs cyber security protection measures imposed by relevant authorities.

10. ENVIRONMENTAL, SOCIAL AND GOVERNANCE

International ESG commitments

Vietnam has made several international climate commitments by signing the United Nations Framework Convention on Climate Change, Vienna Convention for the Protection of the Ozone Layer and COP pledges.

Multilateral agreements include the Cooperation Framework Agreement on Climate Change between Vietnam and the Republic of Korea and the Joint Crediting Mechanism between Vietnam and Japan. Additional climate commitments include NDCs and Greenhouse Gas Emission Reductions.



These international climate commitments are incorporated into domestic law and various legislative and policy measures, such as the Law on Environmental Protection 2020 and Decision No.888/ QĐ-TTg (25 July 2022) which sets out tasks and solutions for implementing outcomes of the 26th Conference of the Parties (COP26) to the UN Framework Convention on Climate Change.

ESG reporting

Publicly listed entities must comply with reporting requirements set out in Circular No. 96/2020/TT-BTC, including by disclosing ESG-related information in their annual reports.

This includes disclosing information regarding greenhouse gas emissions, energy and water consumption, compliance with environmental laws, employee policies and community engagement initiatives.

Renewable energy certificates

Vietnam has two types of tradeable renewable energy certificates (RECs) – international RECs (**I-RECs**) registered by the Green Certificate Company, which make up more than 95% of global REC trading volume, and Tradeable Instrument for Global Renewables (**TIGRs**) registered by APX.

Whether a data centre requires direct renewable power, or just the purchase of relevant RECs will generally be driven by the demands of their anchor tenants. Some hyperscalers may insist on true renewable power supply at site, while others may prefer security of supply from non-renewable sources and instead rely on RECs to meet their internal ESG targets.

11. SECTOR-SPECIFIC REGULATIONS APPLICABLE TO DATA CENTRES

Government bodies

The *Law on Protection of State Secrets 2018* requires government-related data to be securely stored and processed within Vietnam.

The establishment of the government-owned National Data Centre was officially announced in February 2025 by MOPS. The Data Law sets out various requirements for how it will operate. The creation of a National Data Centre was initially contemplated in 2023, in Resolution 175/NQ-CP.

Financial services providers or financial institutions

There are several laws and regulations imposing obligations on entities operating in the financial services sector, such as the *Law on the State Bank of Vietnam 2010*, the *Law on Anti-Money Laundering 2022* and the *Law on Securities 2019*. These laws and regulations impose obligations on financial service providers and institutions - entities that process and manage customer data as part of their regulated business operations.

They **do not**, however, impose obligations on data centre operators where those operators **merely provide the physical infrastructure** (for example, space, power, cooling, and connectivity) without access to, or control over, the data stored on tenant servers.

Digital asset service providers

Digital certification service providers must comply with the Law on Electronic Transactions 2023, and relevant guiding legislation, which (relevantly) set out requirements relating to data storage, processing, and security for digital signatures and authentication services.

These obligations apply specifically to digital certification service providers and **do not extend to data centre operators**, who solely provide physical infrastructure and do not have access to, or control over, the data processed by their tenants.

Digital ID

Digital ID providers must comply with the Law on Citizen Identification 2023, which requires personal identity data to be stored in government-approved data centres.



GLOSSARY

TERM	DEFINITION
5G	5th generation global wireless technology.
AI	Artificial intelligence, which refers to technologies that enable machines to perform tasks traditionally associated with human intelligence, including making predictions, recommendations or decisions.
AI DIFFUSION RULE	AI export control introduced by the Biden Administration which would have imposed a global licensing framework on advanced AI technologies, including advanced AI chips and model weights, introducing ‘tiers’ of access to that technology and various exceptions. The AI diffusion rule was rescinded by the Trump Administration in May 2025.
AI EXPORT CONTROLS	Worldwide restrictions and licensing requirements enforced by the US Bureau of Industry and Security in relation to the export, re-export and transfer (in-country) of certain advanced AI technologies. Controls mostly apply to China and US-embargoed countries after the Trump Administration rescinded the AI diffusion rule.
AI SOVEREIGNTY	The concept that it is in the national interest for a country to control the infrastructure, models, data and skilled workforce required for AI to adapt to its own strategic aims and needs, as AI will be both a key driver of economic growth and a source of national security risk.
AIR COOLING	A method of cooling IT equipment at a data centre using cooling systems at either the room, row or rack level within the data hall.
APAC	Asia-Pacific, which is the geographic region encompassing countries and territories in and adjoining the western Pacific Ocean.
CARRIER	A telecommunications service provider that facilitates the transfer of data or communications – whether fixed or wireless. Typically, a carrier will own or operate the network used for its telecommunications services.
CCTV	Closed-Circuit Television, which is a system that sends television signals to a limited number of screens, often used for security purposes.
CO ₂ E	Carbon Dioxide Equivalent, which is a metric measure used to compare the emissions from various GHGs based on their global warming potential.
CLOUD SERVICE PROVIDER	The provider of highly scalable and flexible computing infrastructure or resources to businesses and organisations.
COLOCATION	Providing space within a data centre for customers to deploy and operate their own IT equipment. Colocation usually comes with power, cooling, connectivity, security and other services.
CORPORATE PHYSICAL PPAS	A corporate offsite physical PPA, or a corporate onsite physical PPA.
CORPORATE PPAS	A corporate offsite physical PPA, a corporate onsite physical PPA or a corporate virtual PPA.
CORPORATE OFFSITE PHYSICAL PPA	A PPA between a consumer and a generator for the physical delivery of electricity to a place outside of the generation site, usually through the grid and accompanied (in the case of renewable electricity and if allowed in the relevant jurisdiction) by the delivery of the environmental attributes associated with the production of renewable electricity.
CORPORATE ONSITE PHYSICAL PPA	A PPA between a consumer and a generator for the physical delivery of electricity to a place on the same site as the generation assets, usually by using low nameplate capacity generation assets such as rooftop PV panels and accompanied (in the case of renewable electricity and if allowed in the relevant jurisdiction) by the delivery of the environmental attributes associated with the production of renewable electricity.

TERM	DEFINITION
CORPORATE VIRTUAL PPA	A PPA between a consumer and a generator for the notional (virtual) delivery of electricity by the generator to a connection point, with the consumer ‘deeming’ the use of such electricity in respect of its own consumption (which may be supplied by an unrelated generator) and accompanied (in the case of renewable electricity and if allowed in the relevant jurisdiction) by the delivery of the environmental attributes associated with the production of renewable electricity.
DATA CENTRE PARK	A purpose-built area or campus designed to accommodate several data centres in close proximity to each other, by providing the infrastructure needed for data centre operation, like power supply and connectivity.
DIGITAL ASSET	An asset that is purely digital (such as a cryptocurrency) or is a digital representation of a physical asset (such as a digital collectible including non-fungible tokens or NFTs).
DIGITAL CERTIFICATION PROVIDER	The provider of an electronic document that verifies the identity of a website, server or individual in online transactions using public key cryptography.
DIGITAL ID	The body of information about an individual that verifies who they are in the digital world, which may include date of birth, email, education qualifications and health information.
ESG	Environmental, Social and Governance, which is a formal framework to measuring and reporting on how a business impacts society and the environment.
FDI	Foreign Direct Investment, the ownership stake in a foreign company or project made by an investor, company or government from another country.
GDP	Gross Domestic Product, the monetary measure of the total value of final goods and services produced by an economy in a given period.
GHG	Greenhouse gases, such as carbon dioxide or methane which, when released into the atmosphere, contribute to the greenhouse effect.
GPU	Graphic Processing Unit, which refers to an electronic circuit designed to handle many tasks at once at a significantly high rate of speed.
GPU-AS-A-SERVICE	A service where companies rent access to powerful GPUs over the internet, instead of buying and maintaining the hardware themselves.
GST	Goods and Services Tax, a tax on the sale of goods and services. It is also referred to as VAT in some jurisdictions.
GW	Gigawatt, which is a unit of power equal to 1,000,000,000 watts.
HOSTING SERVICE PROVIDER	A company that provides remote IT resources and services to enable individuals and organisations to host websites, databases and other critical systems on their servers.
HYPERSCALER	A large-scale, global cloud service provider, such as Amazon Web Services, Google Cloud, Microsoft Azure, AliCloud (Alibaba) and Tencent. Occasionally, global technology companies who do not offer cloud services are referred to as hyperscalers.
HYPERSCALE DATA CENTRE	A data centre that is designed to the specifications of one or more hyperscalers, with substantial computing power and storage capacity.
IEC	International Electrotechnical Commission, a global not-for-profit organisation that publishes international standards for all electrical, electronic and related technologies.
IP	Intellectual Property.
ISO	International Organization for Standardization, which is a non-governmental organisation that develops and publishes standards for different sectors including IT and environmental sustainability.
ISP	Internet Service Provider, which is a company that provides internet access to residential and commercial customers, including data centre operators. An ISP may also be a carrier .
IT	Information Technology.
KV	Kilovolt, a unit of potential difference equal to 1,000 volts.
KVA	Kilovolt ampere, a unit of apparent power in an electric circuit equal to 1,000 volt-amperes.



TERM	DEFINITION
KW	Kilowatt, a unit of power equal to 1,000 watts.
KWH	Kilowatt-hour, a unit of energy measuring the energy transferred or expended by 1KW in 1 hour.
KYC	Know Your Customer, a process used to identify customers and assess their risk, typically conducted in the financial sector.
KYOTO PROTOCOL	An international treaty adopted in 1997 under the United Nations Framework Convention on Climate Change that commits industrialised signatory countries to limit and reduce GHGs in accordance with agreed targets.
LLM	Large Language Model, which refers to an AI system trained on vast quantities of data, often sourced from the internet.
LIQUID COOLING	<p>A method of cooling IT equipment at a data centre using liquids, rather than air. Common liquid cooling technologies include:</p> <ul style="list-style-type: none">• direct-to-chip cooling – where liquids are circulated directly over the surface of the IT equipment (such as a GPU) via a cold plate• immersion cooling – where the IT equipment is submerged in specialised liquids, and• rear door heat exchangers – where the liquid cooling system is attached to the back of the server rack.
LIVE CAPACITY	The amount of data centre capacity available for use in a country, region or area (as the case may be) at any point in time, often measured in MW. This excludes pipeline capacity .
LNG	Liquefied Natural Gas which is a natural gas that has been liquefied by being cooled to extremely low temperatures.
MORATORIUM	A temporary ban or restriction on the development of new data centre in a country, region or area, usually to address concerns about power availability and consumption.
MW	Megawatt, a unit of power equal to 1,000,000 watts.
MWH	Megawatt-hour, a unit of energy measuring the energy transferred or expended by 1MW in 1 hour.
NSP (TELECOMMUNICATIONS)	Network Service Provider, which (in the telecommunications sector) is a telecommunications service provider that provides network services to ISPs and large organisations. A NSP may also be a carrier.
NSP (ENERGY)	Network Service Provider, which (in the energy sector) owns, operates and manages energy (including electricity) networks and infrastructure.
NDC	Nationally Determined Contribution, the national climate action plan by each country under the Paris Agreement.
PARIS AGREEMENT	The international treaty on climate change that was adopted by 195 Parties in Paris, France, on 12 December 2015 and came into force on 4 November 2016.
PIPELINE CAPACITY	The amount of data centre capacity that is under development in a country, region or area at any point in time, often measured in MW. This excludes live capacity .
PPA	Power Purchase Agreement, which is an agreement under which a business will purchase electricity from a supplier at an agreed price over a fixed term.
PRC	People’s Republic of China, references to ‘China’, the ‘Mainland’, ‘Mainland China’ or the ‘PRC’ are references to the People’s Republic of China excluding the Hong Kong Special Administrative Region, the Macao Special Administrative Region and Taiwan.

TERM	DEFINITION
PUE	<p>Power Usage Effectiveness, used to measure the energy efficiency of a data centre, calculated as follows:</p> $PUE = \frac{A}{B}$ <p>Where:</p> <p>A = the total amount of energy used in a data centre B = the energy usage of the data centre’s IT equipment.</p>
REC	Renewable Energy Certificate, a certificate providing evidence that power was generated and delivered to the electricity grid from a renewable energy resource.
SAAS	Software-as-a-Service, cloud-based software distribution model that delivers applications to end-users through an internet browser.
SEZ	Special Economic Zone, a specific geographic location with different regulations or incentives to stimulate economic growth.
UNFCCC	UN Framework Convention on Climate Change, an international environmental treaty established in 1992 aimed at addressing climate change and stabilising GHG concentrations. It provides a framework for negotiating specific international treaties (like the Kyoto Protocol and Paris Agreement) to limit global carbon emissions and promote sustainable development.
VAS	Value-added telecommunication service, which is an additional or ‘add-on’ service that a telecommunications service provider might provide in addition to a traditional telecommunications service. Examples of VAS include caller ID and cloud services.
VASP	Virtual Asset Service Provider, which is an entity that sells, purchases, exchanges, transfers or manages any virtual asset (electronic certificates that have value and can be transferred electronically).
VAT	Value-Added Tax, a consumption tax on the value added in each stage of production for a good or service. Also referred to as GST in some jurisdictions.
WTO	World Trade Organisation.
WUE	<p>Water Usage Effectiveness, a metric to measure data centre sustainability in terms of water usage, as a ratio between the use of water in data centre systems and the energy consumption of its IT equipment, calculated as follows:</p> $WUE = \frac{A}{B}$ <p>Where:</p> <p>A = the total amount of water used in a data centre’s systems B = the energy usage of the data centre’s IT equipment.</p>
ZONING	Laws and regulations that govern how real property can and cannot be used in certain geographic areas, for example, limiting the commercial or industrial use of land.



CONTRIBUTORS



DARYL COX
PARTNER
SINGAPORE
TEL +65 87253595
MOB +65 6991 6506
EMAIL daryl.cox@sg.kwm.com



URSZULA MCCORMACK
PARTNER
SYDNEY
TEL +61 2 9296 2570
MOB +61 429 162 831
EMAIL urszula.mccormack@au.kwm.com



DANIEL CHAN
SENIOR ASSOCIATE
SINGAPORE
TEL +65 6991 6515
EMAIL daniel.chan@sg.kwm.com



EMMA SIMPSON
SENIOR ASSOCIATE
SINGAPORE
TEL +65 6991 6524
MOB +65 8163 1286
EMAIL emma.k.simpson@sg.kwm.com



GALLIEN LEFEVRE
SENIOR ASSOCIATE
HONG KONG
TEL +852 3443 8308
MOB +852 9190 9133
EMAIL gallien.lefevre@hk.kwm.com



CHARLES DAVIES
SENIOR ASSOCIATE
SYDNEY
TEL +61 2 9296 2257
MOB +61 428 918 076
EMAIL charles.davies@au.kwm.com



WESLEY YU
SOLICITOR
MELBOURNE
TEL +61 3 9643 5192
MOB +61 477 902 714
EMAIL wesley.yu@au.kwm.com



THALIA VELEZ RODRIGUEZ
SOLICITOR
MELBOURNE
TEL +65 6991 6559
MOB +61 448 388 058
EMAIL thalia.velezrodriguez@sg.kwm.com



ALEXANDER MCDONALD
LAW GRADUATE
MELBOURNE
TEL +61 3 9643 4369
MOB +61 4 6142 6814
EMAIL alexander.mcdonald@au.kwm.com



GARY SMYTHE
HEAD OF MARKETING
MELBOURNE
TEL +61 3 9643 5351
MOB +61 408 064 429
EMAIL gary.smythe@au.kwm.com



KATIE WALSH
GLOBAL CONTENT AND CAMPAIGNS LEAD
SYDNEY
TEL +61 2 9296 3275
MOB +61 431 759 334
EMAIL katie.walsh@au.kwm.com

We are grateful for those who have shared their insights from across APAC and helped to bring this Guide to life, from KWM 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, Frasers Law Company, Kim & Chang, Romulo Mabanta Buenaventura Sayoc & de los Angeles, Skrine, Trilegal and Tsar & Tsai Law Firm for their collaboration on this guide.

AUSTRALIA

KWM
AARON BROOKS
DAVID ELLIS
INTAN EOW
FRANCESCA GIORLANDO
CHENG LIM
GREG PROTEKTOR
GRACE QIU
CLAIRE ROGERS
ANDREA SHAN
RODERICK SMYTHE
MARK TEH

CHINA

KWM
SUSAN NING
HAN WU
LI ZHUOYAN

HONG KONG

KWM
SCOTT GARDINER
VINCE LEE
GALLIEN LEFEVRE
FRANCOIS TUNG
TIAN XU

INDIA

Trilegal
JISHNU SANYAL
SAMSUDDHA MAJUMDER
AMAR NARULA
KARTIKEY KULSHRESTHA
KURUVILA M JACOB
ATYOTMA GUPTA
ARCHITA SHARMA
ADI KIDAMBI
AFRA ANSARI
ADVETITA

INDONESIA

ABNR
AYIK CANDRAWULAN GUNADI
AGUS AHADI DERADJAT
EMIR NURMANSYAH
MAHISWARA TIMUR
NINA CORNELIA SANTOSO
MOHAMMAD AFIF HIRZI
BEVERLY SHARON LAZA
ADYA SEPASTHIKA
EDMUND KHOVEY

JAPAN

KWM
YOSHIKI TSURUMAKI
TOMOYUKI MIYAZAKI
MUNETOSHI ESAKI
SHUHEI SUGAI

MALAYSIA

Skrine
TAN WEI XIAN
NATALIE LIM
FARIZ BIN ABDUL AZIZ
JESY OOI
RACHEL CHIAH
ENG Y TAN SHIN CHIAN
CHEAM TAT SEAN
SITI AYEENA BINTI MOHD ANIS
BELINDA LIM KE XIN

PHILIPPINES

Romulo Mabanta Buenaventura Sayoc & de los Angeles
PETER PACHECO
AGUSTIN R MONTILLA IV
RAFAEL D DEL ROSARIO
JESSE ELEAZER D TANTOCO

SINGAPORE

KWM
MICHELLE HUANG
MICHAEL LAWSON
PHILIPPA ROBINSON
ELIZA SAVILLE

SOUTH KOREA

Kim & Chang
KYE-SUNG CHUNG
JIN HO SONG
SEUNG HOON YEOM
ARNOLD YOO-HUM BAEK
RICHARD SANG-HOON SUNG
YU SEOK JUNG

TAIWAN

Tsar & Tsai Law Firm
JANICE C.H. LIN
ELLEN PENG
ANTHONY HSIEH

THAILAND

Chandler Mori Hamada
JESSADA SAWATDIPONG
PANUPAN UDOMSUVANNAKUL
SARUNPORN CHAIANANT
KORAPHOT JIRACHOCKSUBSIN

VIETNAM

Frasers Law Company
HO THUY NGOC TRAM
MARK FRASER
HOANG THI THUY VY
TRAN LE MINH TRUC

TAG

ABRAHAM ALVAREZ
SACHIE HEWA KADAWEDDUWAGE
DAMIEN WINDOW

Many people contributed to this publication and we are deeply grateful to them all.

KWM

DESMOND CAI
JAY DING
MATILDA ELLIOTT
JUSTIN FEI
CLARIS FOO
ELLA HALL
WINSTON LI

STEFANO MASCARO
ALEX MEI
JOY MIDUKU
MELISSA MOONEY
AOIFE RHATIGAN
ELLIE RITTER
NADIA WUST





ABOUT KING & WOOD MALLESONS

A firm born in Asia, underpinned by world class capability. With over 3,700 lawyers in 26 global locations, we draw from our Eastern and Western perspectives to deliver incisive counsel.

We help our clients manage their risk and enable their growth. Our full-service offering combines un-matched top tier local capability complemented with an international platform. We work with our clients to cut through the cultural, regulatory and technical barriers and get deals done in new markets.

Disclaimer

This publication provides information on and material containing matters of interest produced by King & Wood Mallesons. The material in this publication is provided only for your information and does not constitute legal or other advice on any specific matter. Readers should seek specific legal advice from KWM legal professionals before acting on the information contained in this publication.



JOIN THE CONVERSATION



SUBSCRIBE TO OUR WECHAT COMMUNITY.
SEARCH: KWM_CHINA

Asia Pacific | North America

King & Wood Mallesons refers to the network of firms which are members of the King & Wood Mallesons network. See kwm.com for more information.

www.kwm.com

© 2025 King & Wood Mallesons

