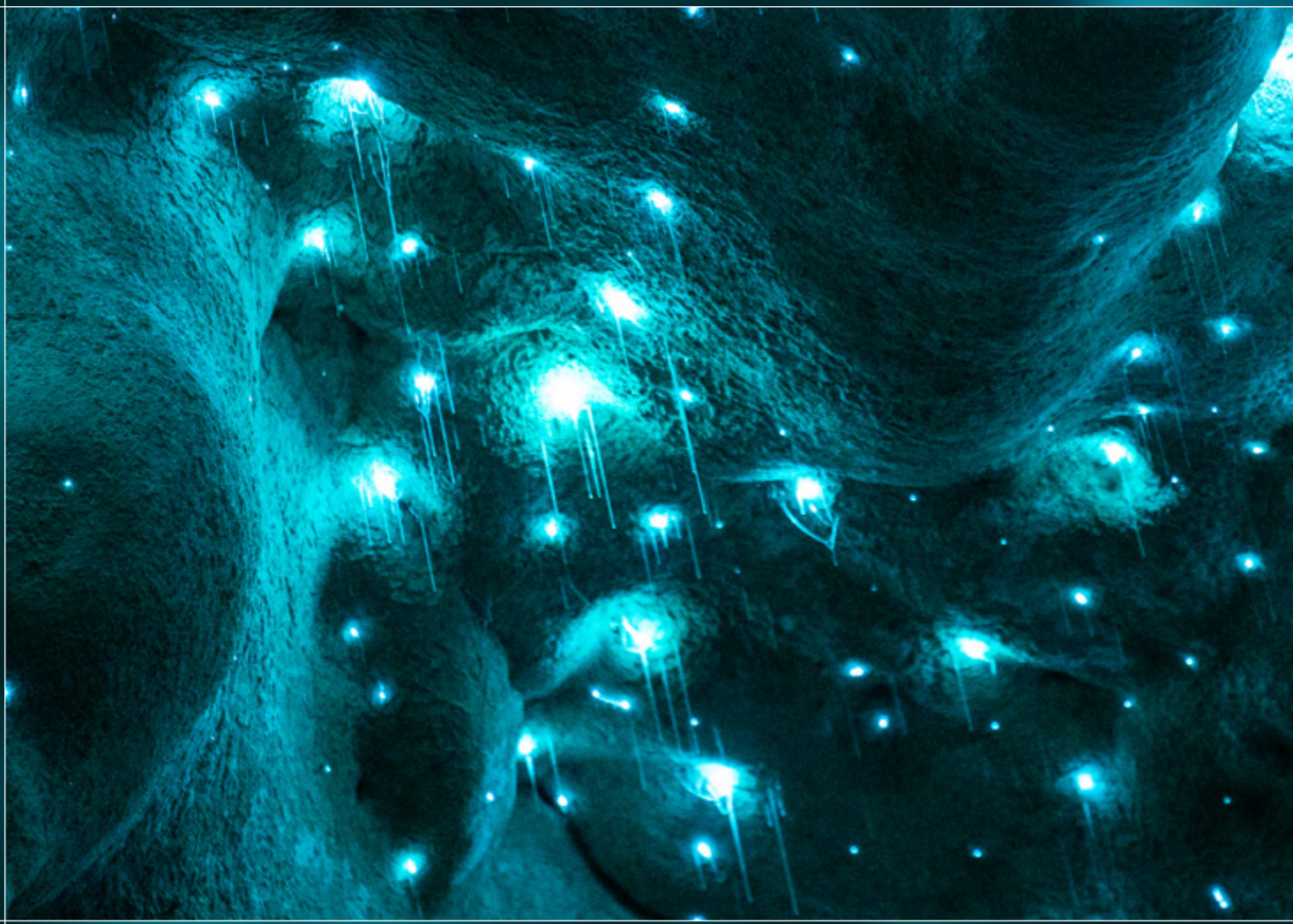
November 2026

Data Centres

APAC Regulatory Guide – **India**

Investment considerations



MALLESONS

Chapter 4

India

A year of... surging capacity, cleaner power procurement and a maturing regulatory framework

Population
1.48
billion

Data centres
295
YoY: 26 (9.7%)

Live capacity
1.73GW
YoY: 119MW (7.4%)

Pipeline capacity
3.81GW+
YoY: 388MW (11.3%)

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

India's data centre industry is experiencing rapid growth. Live capacity is expected to reach 3GW+ by 2028, driven by digital transformation, favourable government policies and strong 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

- Data storage demand 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 *Telecommunications Act 2023* (**Telco Act**) establishes a new framework for the regulation of telecommunications networks and services, which may be relevant to data centre operators supporting telecommunications infrastructure and services. A number of the operative portions of the Telco Act have been brought into force by way of the related notification of operational rules.
- The *Digital Personal Data Protection Act 2023* (**DPDP Act**) introduces new data protection requirements across the board and will be effective from May 2027.
- Targeted data localisation requirements in sectors like financial services and telecommunications are prompting companies to expand local storage capacity.

> 'India is fast becoming a major destination for data centre investment. Long-term tax incentives, expanding digital infrastructure and a maturing regulatory framework are strengthening the investment environment. As AI drives demand for compute capacity, early compliance planning will be critical for organisations looking to set up and grow operations in India.

Jishnu Sanyal
Partner, Trilegal



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**).

DisComs are subject to a Universal Service Obligation (**USO**) under the Electricity Act, requiring them to provide an electricity connection to any applicant who meets the necessary commercial and technical conditions.

The DisCom cannot refuse supply of a connection even where grid extension or augmentation is required.

Upon approval of a connection, 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**).

Proposed amendments to the Electricity Act

Draft amendments have been proposed to the Electricity Act which would allow the SERC to, in consultation with the relevant state governments, remove the USO requirement for large consumers with more than 1MW contract demand and who are already eligible to procure power through open access from retailers, or through the power exchange.

In those instances, large consumers would be expected to make their own power procurement arrangements without relying on DisComs. Alternatively, the draft amendments provide that the SERC may designate a DisCom to act as a 'supplier of last resort' and provide supply at a premium over cost of supply to a large consumer if unable to procure power under other supply arrangements.

Separately, data centre consumers may procure power for their facilities on an intrastate or interstate basis from retailers (that is, independent power producers) and captive generation plants. Such arrangements require additional approvals, typically taking 4 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, where generation assets are located on the premises of the end user or 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 for the supply of power from an inter-state grid connected to 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 now possible, pursuant to the notification of the Central Electricity Regulatory Commission's 'Guidelines for Virtual Power Purchase Agreements' from 2025, which require virtual PPAs to be structured as non-transferable and non-tradeable contracts for the delivery of domestically recognised renewable energy credits.

Corporate virtual PPAs which do not follow those Guidelines may be classified as 'commodity derivatives'.



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 this, 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.

'DisCom' status for private companies

In April 2026, Google, through its subsidiary Raiden Infotech, became the first private company in India to be granted a deemed 'DisCom' licence for its proposed 1GW data centre campus in Vishakhapatnam, Andhra Pradesh.

As a deemed 'DisCom', Raiden Infotech can procure electricity, either conventional or renewable, directly from power generators in India rather than procuring it through a DisCom, enabling internal distribution of power across its data centre facilities in Vishakhapatnam and providing greater long term cost certainty.

Uttar Pradesh's Data Centre Policy 2021 allows data centre park operators and developers to obtain a deemed 'DisCom' licence to procure, and supply, power for their facilities.

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

These are 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

Where can developers build data centres?

Data centres in India must be developed on land designated for commercial, industrial or non-agricultural use. Land is classified under state revenue records as agricultural, industrial, residential, commercial or forest. Developers must ensure the identified land is appropriately zoned to avoid future regulatory issues.

Although foreign entities are generally prohibited from directly acquiring land (as 'immovable property') in India unless they establish a local presence, this does not apply to data centre development. As a result, land acquisition by foreign entities for data centre development is generally permitted (see 'Foreign investment restrictions' below for further details).

Are any permits or approvals required?

To develop and operate a data centre in India, developers must secure multiple state-specific permits. These include:

- building plan approvals
- commencement and occupancy certificates
- pollution and fire safety clearances
- water supply permissions, and
- approvals for tree felling and waste disposal.

Timelines vary by local jurisdiction, and delays can result from title issues, land disputes or procedural inefficiencies.

What if rezoning or changes to covenants are needed?

If the land identified is not already zoned for commercial or industrial use (data centres are classified as 'communication' sector infrastructure entities), rezoning is required.

- If land is classified as agricultural, a land conversion order must generally be obtained from the relevant state authority. Failure to obtain conversion can result in penalties, including fines, and in some cases, land confiscation. Conversion orders typically take 3 to 6 months, though timelines vary by state.

  In some states, such as Madhya Pradesh, operators can provide an initial post-acquisition notification and obtain the land conversion order following the acquisition.

Additionally, most states impose landholding ceilings on agricultural land - usually 20 to 100 acres - requiring prior exemptions if a developer exceeds the threshold.

- If the land is classified as forest, central and state government approvals are required for leasing or repurposing it for non-forest use.

  This process can take 60 to 120 days and involves conditions such as compensatory afforestation, which must be fulfilled before final approval is granted.

04 Telecommunications

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

While data centre developers and operators in India were not ordinarily required to hold a telecommunications licence, as they were not considered telecommunication service providers under the *Telegraph Act 1885*, this will need to be re-examined under the Telco Act.

The Telco Act, which came into force on 23 June 2026, introduces broader definitions for 'telecommunication service' and 'telecommunication network', and introduces new categories of authorisations. In particular, the introduction of a new category of authorisation for 'cloud-hosted telecommunication network providers' means that data centre operators may now be subject to authorisation requirements depending on the nature of the services they provide customers.

Applicability of telecommunications laws to data centres

Under the *Telecommunications (Authorisation for Telecommunication Network) Rules 2026* (**Network Authorisation Rules**), a 'cloud-hosted telecommunication network' (**CTN**) is defined as a telecommunication network built using cloud computing principles, which virtualises network functions and runs them as software on standard hardware. In turn, 'cloud-hosted telecommunication network as a service' (**CTNaaS**) includes provision to an authorised telecommunication entity/licensee of:

- physical infrastructure for housing cloud-hosted telecommunication equipment
- cloud-hosted telecommunication equipment for use in a telecommunication network, and
- cloud-hosted telecommunication network functionality for provision of telecommunication services.

A data centre provider may be subject to authorisation requirements where it is, in substance, providing infrastructure or functionality that forms part of a cloud-hosted telecommunication network used for provision of telecom services.

This is relevant because 'physical infrastructure' is defined to include infrastructure such as:

- buildings
- passive telecommunication infrastructure, and
- right of way held by the provider or its facility provider.

The analysis therefore turns on what is actually being offered. Bare real estate/generic hosting may not by itself trigger authorisation, but provision of infrastructure for housing cloud-hosted telecommunication equipment, or provision of telecommunication-facing virtualised network functionality, may do so.

A CTN authorisation permits a data centre to support licensed telecommunication operators in up to three ways:

- by hosting the operator's network equipment on its premises
- by supplying that equipment itself, and
- by providing network functions as software running on its cloud infrastructure.

A data centre may offer all three as a combined CTNaaS offering.

A CTN provider may only serve other authorised entities or licensees — it cannot itself provide the underlying telecommunication service to end users. Where a data centre wishes to provide telecommunication services directly to users, a separate service authorisation will be required.

Captive networks

The *Telecommunications (Authorisation for Captive Telecommunication Services) Rules, 2026* provide for a captive non-public network (**CNPN**) authorisation, permitting an authorised entity to establish, operate, maintain or expand a private network within the logical perimeter of premises occupied by it.

One CNPN authorisation can cover several sites. The operator must notify the Department of Telecommunications of the location of each additional site. A CNPN authorisation gives no right to spectrum, which must be leased from an access provider or obtained from the government, separately for each site.

Further, a CNPN cannot be used for any commercial or public telecommunication service or connect to public telephone, mobile or internet networks. Sites may be linked only through domestic leased circuits from a licensee and each CNPN must operate within the premises.

Accordingly, a CNPN authorisation provides a regulatory framework for closed, captive communications within a data centre and, where required, across multiple data centre sites within the same premises.

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*.

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
- limited liability partnership (see 'Land' above for further details).

Even then, foreign entities 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 FDI restriction for data centre development is for investments where the beneficial owner is situated in, or is a citizen of, any country sharing a land border with India. These are China, Bangladesh, Pakistan, Bhutan, Nepal, Myanmar and Afghanistan.

Investments from those in restricted countries require prior approval of the Indian government.

To unlock greater FDI inflows, the Non-Debt Rules were recently amended in May 2026 to relax the definition of 'beneficial ownership' and expedite approval timelines.[1]

For more details, see '[Easing of FDI restrictions on investments from land border sharing countries]'.

Telecommunications

India generally permits up to 100% FDI in sectors like telecommunications, broadcasting, manufacturing and infrastructure under the Non-Debt Rules. However, FDI from restricted countries requires prior government approval, subject to the limited changes outlined above.

06 Tax and other incentives

Special economic zones

India has established several special economic zones (**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 the SEZs established in 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

To attract investment in AI and data centre infrastructure in India, the Indian government has introduced two key changes effective from 1 April 2026.

- **Tax holidays**

  For a period up to 31 March 2047, a tax holiday is available to foreign companies in relation to income accruing or arising in India, or deemed to accrue or arise, by way of procuring any data centre service from specified data centres, operated by Indian companies (whether by way of owning or leasing) where it accrues, arises or is deemed to accrue or arise in India.

  Certain conditions must be met, including the foreign company not owning or operating any physical infrastructure or resources of the specified data centre and where services are provided to Indian customers, the foreign company must route the sale through an Indian reseller entity (being an Indian company).

- **Safe Harbour Regime**

  Data centre services provided by an Indian entity to a related foreign company fall within the safe harbour regime for transfer pricing purposes, so that an Indian data centre that is providing services to foreign entities within its corporate group can apply a fixed 15% margin on its costs for income tax purposes.

In addition to these measures, 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, with the latest round of stakeholder consultation reported in September 2025.

07 Data protection and cyber security

Data protection or privacy laws

India's data protection laws apply to 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* (**SPDI 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 DPDP Act (effective in May 2027) introduces broader obligations for entities controlling personal data (called 'data fiduciaries'), including implementing reasonable security safeguards set out in the Act and supporting rules.

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 address allocation, timestamps, purpose of service and ownership details, and
- clock synchronisation with authorised Indian Network Time Protocol servers.



1. Please refer to: https://trilegal.com/knowledge_repository/trilegal-update-easing-of-fdi-restrictions-on-investments-from-land-border-sharing-countries/

Government sector

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 institutions sector

Entities regulated by the Reserve Bank of India (RBI) who outsource IT services, including to data centre operators, 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.

Synchronisation with Indian Standard Time (IST)

The *Legal Metrology (Indian Standard Time) Rules 2026*, which come into force on 26 February 2027, establish additional time-synchronisation requirements for specific critical sectors like data centres.

Data centres must synchronise time-dependent systems to IST using an authorised timing source traceable to Coordinated Universal Time maintained by the National Physical Laboratory of India, such as:

- the National Physical Laboratory of India
- a Regional Reference Standard Laboratory, and
- Navigation with Indian Constellation or the National Informatics Centre.

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, being:

- systems whose failure would severely impact national security, the economy, public health or safety, or
- across key sectors including 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. Designated data centres must comply with strict security protocols, including the establishment of cyber security and network operations centres.

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*. 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.

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

Limited data localisation requirements

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

Nevertheless, data fiduciaries designated by the government as 'significant data fiduciaries' must localise certain personal data and traffic data within India. No notification has been made in this regard to date.

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.

Additionally, all data centre operators, 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.

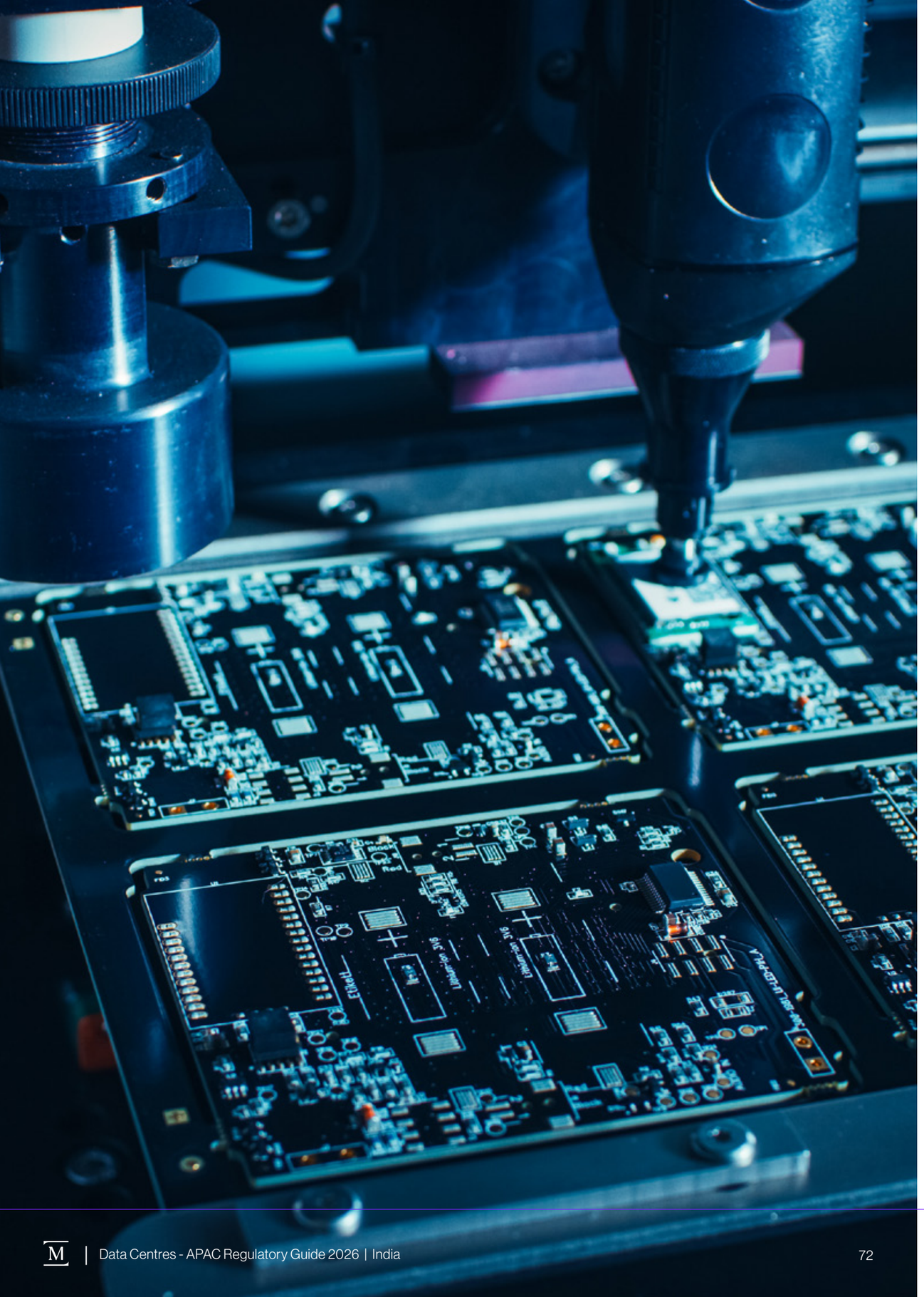


Sector-specific localisation restrictions currently in place

- **Financial services:** The 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 - while processing abroad is permitted, 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.
- **Telecommunications:** Licensed telecommunications service providers must store subscriber data, accounting information, network logs and IP address records within India and are generally prohibited from transferring this data overseas, except in limited cases such as international roaming or to comply with legal requirements.

  The Network Authorisation Rules separately require authorised entities providing CTNaaS to store locally, all systems of the telecommunication network and associated data, logs and information, with no copies routed, shared or made available outside India.

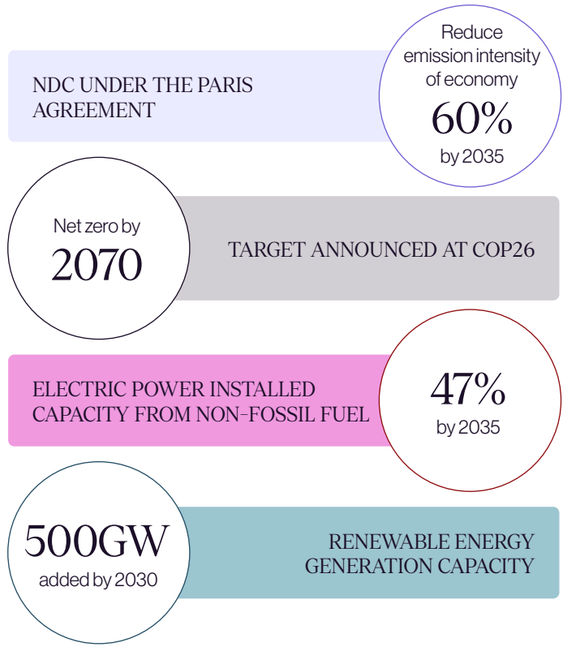
  Remote access to the telecommunication network from outside India requires prior Central Government approval and is subject to prescribed safeguards. These requirements may be directly relevant to data centre operators where activities fall within the scope of the Network Authorisation Rules, including under CTN authorisations.



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 and 2026.



Environmental requirements

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

While the Draft Data Centre Policy, released in 2020 by the Ministry of Electronics and Information Technology, 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 government 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.

The Indian government is reportedly in the process of introducing a National Data Centre Policy based on industry wide consultations undertaken in 2025. Therefore, these requirements may be revised in the near future.

Voluntary standards

The Bureau of Indian Standards, India's national standards body, has adopted and introduced voluntary standards on data centre facilities, infrastructure and key performance indicators, covering topics such as:

- building construction
- power distribution
- environmental control
- security systems
- cooling efficiency ratio
- carbon usage effectiveness, and
- water usage effectiveness.

The standards are currently voluntary in nature, but may become binding if specifically notified as such by a sectoral regulator (such as the Department of Telecommunications, or Ministry of Electronics and Information Technology) or incorporated into applicable law.

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 the Securities and Exchange Board of India's mandatory reporting of ESG data (including carbon emissions) for the top 1,000 listed companies.

Contributors



Daryl Cox

PARTNER
SINGAPORE

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



Aaron Ong

SENIOR ASSOCIATE
SINGAPORE

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



Daniel Chan

SENIOR ASSOCIATE
SINGAPORE

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



Charles Davies

SENIOR ASSOCIATE
SYDNEY

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



Wesley Yu

ASSOCIATE
SINGAPORE

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



Thalia Velez Rodriguez

SOLICITOR
MELBOURNE

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



Samantha Gates

SOLICITOR
MELBOURNE

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



Charlotte Hartley

SOLICITOR
MELBOURNE

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



Gary Smythe

HEAD OF MARKETING – CONTENT & CAMPAIGNS
MELBOURNE

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



Katie Walsh

CONTENT & CAMPAIGNS LEAD
SYDNEY

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

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

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

Australia

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

China

King & Wood
Susan Ning
Han Wu

Hong Kong SAR

King & Wood
Tian Xu
Scott Gardiner
Vince Lee
Francois Tung

India

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

Indonesia

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

Japan

Mori Hamada & Matsumoto
Satoru Hasumoto

Malaysia

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

New Zealand

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

Philippines

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

Singapore

Mallesons
Daryl Cox
Daniel Chan
Wesley Yu
Aaron Ong
Charlotte Handley

South Korea

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

Taiwan

Lee and Li
Lily Kuo
Sarah Wu
Chi Lee
Helen Huang

Thailand

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

Vietnam

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

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

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

About Mallesons

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

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

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

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

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

Join the conversation

mallesons.com

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