argus partners
SOLICITORS AND ADVOCATES

POWERING THE DIGITAL DECADE: A GUIDE TO SETTING UP DATA CENTRES IN INDIA

November 2026



MUMBAI | DELHI | BENGALURU | KOLKATA

I. OVERVIEW

The rapid adoption of artificial intelligence ("**AI**"), cloud computing, digital payments, 5G connectivity and data-intensive enterprise applications is fundamentally changing the infrastructure requirements of India's digital economy. AI workloads need far more computing power, storage and high-speed networking than conventional enterprise applications. As a result, the demand for physical infrastructure capable of hosting high-density computing workloads is increasing alongside the growth in data generation and digital consumption.

India generates nearly one-fifth of global data, while the country has historically accounted for only a relatively small proportion of global data-centre capacity.[1] This mismatch between data generation and domestic storage and processing capacity is an important structural driver for further investment in data-centre infrastructure.

The Indian market has consequently moved from being principally a market for conventional enterprise data centres towards a market increasingly characterised by hyperscale campuses, cloud infrastructure, and AI-ready facilities. As of 2026, India has more than 150 (one hundred fifty) data centres with approximately 1.8 (one point eight) GW of operational capacity and is expected to reach 8 (eight) GW by 2030 as AI-ready infrastructure expands.[2] India also received USD 173 billion (United States Dollars one hundred seventy-three billion) of cumulative data-centre investment commitments between 2021 and H1 2026, including approximately USD 38 billion (United States Dollars thirty-eight billion) announced during H1 2026.[3] This expansion creates unprecedented opportunities across construction, power infrastructure, cooling technology and IT equipment sectors.

II. MARKET SIZE AND INCREASING INVESTMENT ACTIVITY IN INDIA

India's data-centre market is expanding rapidly, with Mumbai, Chennai, Delhi-NCR and Bengaluru emerging as the major hubs due to their connectivity infrastructure, submarine cable landing stations and established data-centre ecosystems. As of December 2025, India's operational data-centre capacity had reached approximately 1.5 (one point five), up from around 375 (three hundred seventy-five) MW in 2020, with Mumbai alone accounting for about 790 (seven hundred ninety) MW.[4]

The market is also beginning to expand geographically. Developers and hyperscalers are increasingly considering locations such as Andhra Pradesh and other Tier-II markets, where land and power availability, renewable-energy potential and scope for large campuses can support AI-oriented infrastructure. The sector comprises global hyperscalers, telecom operators, domestic data-centre platforms and infrastructure investors, with significant capital already deployed alongside substantial new investment commitments. For example:

---

[1] Council on Energy, Environment and Water (CEEW), *How is Data Centre Infrastructure in India Shaping Power and Water Use*, available at: https://www.ceew.in/publications/how-is-data-centre-infrastructure-in-india-shaping-power-and-water-use, accessed on November 18, 2026.

[2] Cushman & Wakefield, *India Data Centre H1 2026 Update*, September 2026, available at:https://www.cushmanwakefield.com/en/india/news/2026/09/india-data-centre-h1-2026-update; ET Data Centres, *India's Data Centre Capacity Projected to Reach 8 GW by 2030*, available at: https://datacenters.economictimes.indiatimes.com/news/market-insights-analysis/indias-data-centre-capacity-projected-to-reach-8-gw-by-2030/134250756, accessed on November 18, 2026.

[3] CBRE, *Beyond Growth: India's Rise as a Global Data Centre Hub*, available at: https://mktgdocs.cbre.com/2299/a82bb1ff-ef8f-4d85-aced-b79c4783b244-1835070418/Beyond_Growth_-_India_s_Rise_A.pdf, accessed on November 18, 2026.

[4] Press Information Bureau, Government of India, *Press Release*, available at: https://www.pib.gov.in/PressReleaseDetail.aspx?PRID=2241783&reg=1&lang=1, accessed on November 18, 2026.

- Amazon has invested more than USD 3.7 billion (United States Dollars three point seven billion) in cloud infrastructure in Maharashtra between 2016 and 2022,[5] and more than USD 1.3 billion (United States Dollars one point three billion) in its cloud infrastructure in Hyderabad by the end of 2025.[6] Further, in June 2026, Amazon announced an additional USD 13 billion (United States Dollars thirteen billion) investment in AI and cloud infrastructure in India by 2030, which will support the expansion of AWS data centre infrastructure in Mumbai and Hyderabad.

- Google / AdaniConneX / Nxtra: Google has announced an investment commitment of approximately USD 15 billion (United States Dollars fifteen billion) for AI infrastructure in Visakhapatnam, Andhra Pradesh, to be deployed between 2026 and 2030. The project includes a gigawatt-scale data-centre campus, large-scale energy infrastructure and expanded fibre connectivity, and is being developed in collaboration with AdaniConneX and Nxtra by Airtel.[7]

Other significant operators include NTT, ST Telemedia Global Data Centres, Yotta, CtrlS, Sify, Equinix, and Princeton Digital Group.

III. BUSINESS MODELS

The Indian data-centre market has a range of ownership and service models, which broadly depend on whether the facility is developed for the exclusive use of an enterprise or is operated by a third-party provider for multiple customers. Within outsourced infrastructure, the principal models are colocation, hosting, and hybrid services. These models may coexist within the same data-centre campus and have different implications for capital expenditure, operating responsibility, contract tenure, and risk allocation.

India's data-centre market is predominantly third-party operated, with captive (enterprise-owned) facilities accounting for a relatively small share. It is estimated that enterprise-owned facilities account for ~15% (fifteen percent) of India's data-centre infrastructure.[8] Unlike mature Western markets, India has developed a relatively limited base of captive facilities and has moved towards a colocation-led model, which now supports the expansion of hyperscale and AI infrastructure. This shift is expected to continue as enterprises, particularly in the Banking, Financial Services and Insurance (BFSI) and ITeS sectors, move legacy captive infrastructure to colocation facilities to meet regulatory requirements (*as discussed in Section VI (C) below*) and achieve cost efficiencies.

(A) CAPTIVE MODEL

Under the captive model, an enterprise builds, owns, operates and maintains a data centre for its own use. The facility is designed around the enterprise's specific workloads, security requirements, infrastructure configuration and operational needs. The principal benefit is control: the enterprise can determine the architecture, technology stack, security protocols, physical access arrangements, data environment and operating policies without depending on a third-party facility operator. A captive model may be suitable where an enterprise has specific

[5] Amazon Press Centre, *AWS to invest INR 1,05,600 crores (US $12.7 billion) into cloud infrastructure in India*, May 18, 2023, available at: https://press.aboutamazon.com/in/2023/5/aws-to-invest-inr-1-05-600-crores-us-12-7-billion-into-cloud-infrastructure-in-india, accessed November 18, 2026.
[6] Amazon News, *AWS to expand data centre operations in Hyderabad*, July 15, 2026, available at: https://www.aboutamazon.in/news/aws/aws-data-centre-hyderabad, accessed November 18, 2026.
[7] Google India, *Our First AI Hub in India, Powered by a $15 Billion Investment*, October 14, 2025, available at: https://blog.google/intl/en-in/company-news/our-first-ai-hub-in-india-powered-by-a-15-billion-investment, accessed November 18, 2026.
[8] Mordor Intelligence, *India data center market size & share analysis - Growth trends and forecast (2026 - 2031)*, available at https://www.mordorintelligence.com/industry-reports/india-data-center-market, accessed November 18, 2026.

infrastructure needs, predictable long-term capacity requirements, or wants greater control over its critical infrastructure.

The principal disadvantages of this model are the capital expenditure and operational responsibilities associated with owning the facility. The enterprise must fund land and construction, power and cooling infrastructure, IT equipment and ongoing maintenance, while also maintaining specialist personnel and security capabilities.

(B) OUTSOURCED / THIRD-PARTY MODEL

Under an outsourced model, a specialised data-centre operator develops and operates the facility and provides infrastructure or related services to customers. This allows customers to avoid the upfront capital expenditure and operational burden associated with developing and maintaining a data-centre facility, while benefitting from specialist power, cooling, connectivity, security, and scalable capacity. The principal trade-offs are reduced direct control over the physical infrastructure and dependence on the provider's service quality and availability.

The model is particularly relevant to enterprises for which operating data-centre infrastructure is not a core business function. These include users such as BFSI entities, telecom companies, retailers, media and entertainment businesses, e-commerce companies, cloud service providers and content delivery networks. The outsourced model broadly comprises colocation, hosting and hybrid models, as described below:

(i) **Colocation**: Under a colocation model, the customer leases space and associated facility capacity in a third-party data centre and deploys its own IT equipment. The operator provides the underlying facility infrastructure, including power, cooling, connectivity, backup and physical security, while the customer retains control of its IT environment. Colocation is suited to customers that require high-availability infrastructure and connectivity but wish to retain control over their own equipment. It is used across cloud services, BFSI, media and entertainment, and e-commerce, and is increasingly used by enterprises transitioning from captive infrastructure.

(ii) **Hosting/Cloud:** In addition to colocation facilities, data centre operators or third-party service providers may offer hosting services, under which customers obtain access to servers, storage, computing capacity or related IT infrastructure without deploying their own equipment. The service provider may therefore assume responsibility for a greater portion of the infrastructure stack, including the provision and maintenance of IT equipment housed within its own or third-party colocation facilities. Hosting is generally suited to customers seeking lower infrastructure capital expenditure, rapid scalability and reduced requirements for in-house infrastructure management, but involves greater reliance on the provider's systems and service arrangements.

(iii) **Hybrid:** Under a hybrid model, an enterprise combines its captive infrastructure with colocation and hosting services. The enterprise retains control over its captive infrastructure and may also deploy its own equipment in colocation facilities, while relying on service providers to supply or manage infrastructure and services for ancillary workloads. This model is particularly relevant where an enterprise retains legacy or dedicated workloads on its own infrastructure while migrating other workloads to cloud or colocation facilities. The principal benefit of a hybrid model is flexibility: an enterprise can retain control over workloads that require dedicated infrastructure while outsourcing other workloads and operational functions. However, effective implementation requires a clear allocation of responsibility across infrastructure, applications, security, connectivity and service management.

IV. POLICY AND INCENTIVES FRAMEWORK

(A) DRAFT DATA CENTRE POLICY 2020

The Ministry of Electronics and Information Technology ("**MeitY**") had released the Draft Data Centre Policy, 2020 ("**Draft Policy**"), setting out a comprehensive framework for positioning India as a globally competitive data-centre hub. The Draft Policy envisages the development of data centre economic zones and parks, a data centre incentivisation scheme, fiscal and non-fiscal incentives, single-window clearances, and institutional mechanisms including a Data Centre Facilitation Unit and Data Centre Industry Council. It also identifies key infrastructure requirements, including reliable and uninterrupted power supply, captive generation, open access, renewable-energy procurement, multi-path fibre connectivity, access to national fibre infrastructure and streamlined right-of-way approvals.

A significant subsequent development was the inclusion of data centres in the Harmonised Master List of Infrastructure Sub-sectors in 2022. This classification facilitates greater access to credit for digital infrastructure. The infrastructure classification operates alongside the policy framework contemplated under the Draft Policy.

(B) UNION BUDGET 2026

The Union Budget 2026, followed by the Finance Act, 2026, introduced tax measures to promote India as a global data-centre and cloud-services hub by offering the following incentives:

(i) **Safe-harbour regime**: An Indian data-centre service provider supplying cloud services to a related foreign company outside India can opt for a 15% (fifteen percent) safe-harbour margin for transfer-pricing purposes.

(ii) **Tax holiday up to March 31, 2047:** A qualifying foreign company can avail itself of a tax holiday on income arising from procuring data-centre services in India from a 'Specified Data Centre'.[9] The foreign company must (i) be specifically designated by the Central Government as an eligible entity for tax exemption; (ii) not own or operate the data-centre infrastructure; (iii) route all sales to users located in India through an Indian reseller entity; and (iv) comply with prescribed reporting requirements.

(C) STATE LEVEL INCENTIVES

Along with the Draft Policy released by the central government, several states in India, including Gujarat, Karnataka, Telangana, Uttar Pradesh, Haryana and Maharashtra have introduced dedicated data-centre policies to promote investment in the sector and facilitate development of data centre infrastructure. The state policies provide incentives across areas within state jurisdiction, including land, stamp duty, electricity, power infrastructure, renewable energy, building regulations, water and local approvals. The key incentives offered under these policies are provided below:

(i) **Land:** State policies provide for concessional allotment or long-term leases of land owned by the government or industrial development authorities, land subsidies, exemptions from land conversion charges and stamp duty concessions on land acquisition and lease transactions. For instance, the Uttar Pradesh Data Centre Policy, 2026 provides land subsidies of 25% (twenty-five percent) on prevailing sector rates in Madhyanchal and Paschimanchal and 50% (fifty percent) in Bundelkhand and Purvanchal for eligible land purchased or leased from state agencies.[10] Similarly, the

[9] Under the Finance Act, 2026, Specified Data Centre is defined as a data centre which is established under a MeitY-approved scheme, and owned and operated by an Indian company.
[10] Paragraph 7.1.3 of UP Data Centre Policy, 2026.

Karnataka Data Centre Policy provides a 10% (ten percent) subsidy on land purchase or lease, subject to specified limits, and a 100% (one hundred percent) stamp duty exemption for eligible projects outside Bengaluru Urban district.[11]

(ii) **Power Infrastructure:** Given the significant electricity requirements of data centres, state policies provide incentives to reduce power procurement costs and facilitate reliable electricity supply. These include electricity-duty exemptions, power tariff concessions, open-access procurement of renewable energy, and waivers or reimbursements of transmission and wheeling charges. For example, Gujarat's Viksit Gujarat Data Centre Policy provides power tariff reimbursement of Rs. 1 (Rupees one) per unit for 20 (twenty) years from commencement of commercial operations.[12] The Karnataka Data Centre Policy permits eligible data centres outside Bengaluru Urban district to access industrial power tariffs, subject to a minimum green-energy consumption requirement.[13] Rajasthan's Data Centre Policy, 2025 also provides concessions relating to captive renewable power, subject to certain conditions.[14]

(iii) **Fiscal incentives:** States offer financial support to reduce the initial capital outlay and, in certain cases, ongoing operating expenditure. These measures include subsidies linked to eligible fixed capital investment, interest subsidies, reimbursement of eligible state goods and services tax (SGST), and operating expenditure reimbursements. For instance, the Uttar Pradesh Data Centre Policy, 2026 provides a capital subsidy of 7% (seven percent) of eligible fixed capital investment, capped at Rs. 20 crore (Rupees twenty crore), subject to specified conditions[15]. Odisha's State Data Centre Policy, 2022 provides a capital subsidy of 20% (twenty percent) of fixed capital investment, excluding land costs, capped at Rs. 25 crore (Rupees twenty-five crore) per data centre unit, along with reimbursement of eligible net SGST for up to seven years[16]. Haryana's Data Centre Policy, 2026 provides capital expenditure support of 20% for hyperscale data centres, capped at INR 25 crore per unit, and 10% (ten percent) for core data centres, capped at Rs. 1 crore (Rupees one crore) per MW[17]. It also provides reimbursement of a portion of eligible operating expenditure for five years, subject to specified annual caps.

(iv) **Other incentives and facilitation measures**: State policies also provide non-financial support to facilitate project development and operations. These measures include dual-grid power supply infrastructure, single-window mechanisms for statutory approvals, relaxed building and development norms, enhanced floor space index (FSI), water infrastructure, and employment and training incentives. For example, Maharashtra's IT-ITeS Policy, 2023 permits data centres across different land-use zones and provides for relaxed building norms, including those relating to FSI and building height. Such measures can support project execution and operational resilience, in addition to the direct financial benefits available under state policies.

State-level policy incentives offer clear advantages, but their real-world value must be weighed against core operational expenses like power, cooling, water, and high-speed connectivity. Successful deployment also depends on meeting key compliance criteria, which may include formal eligibility certifications, timely filings, minimum investment thresholds, job-creation commitments, and operational timeline targets.

[11] Paragraph 4.5 of Karnataka Data Centre Policy, 2022.
[12] Paragraph 6.1 of Viksit Gujarat Data Centre Policy, 2026.
[13] Paragraph 4.8 of Karnataka Data Centre Policy, 2022.
[14] Paragraph 4.6.4 of Rajasthan Data Centre Policy, 2025.
[15] Paragraph 7.1 of Uttar Pradesh Data Centre Policy, 2026.
[16] Paragraph 13.1.3 of Odisha State Data Centre Policy, 2022.
[17] Paragraph 9.1 A of Haryana Data Centre Policy, 2026.

V. KEY CONSIDERATIONS FOR SETTING UP A DATA CENTRE IN INDIA

The growth opportunity of data centres must be assessed alongside the resource intensity and infrastructure requirements of data-centre operations. Substantial upfront capital expenditure including land acquisition or leasing costs, stamp duty, registration charges, property taxes, and site development and infrastructure costs must also be considered. While state-specific incentives (*as discussed in Section IV(C) above*) may mitigate some of these costs, site selection should extend beyond the initial land cost. The key considerations are discussed in greater detail below.

(A) SITE SELECTION – LAND, ZONING AND INFRASTRUCTURE

The selection of a suitable site is a critical consideration and requires assessment of title, land use, zoning, development potential, power, water, fibre connectivity, environmental constraints, physical access and future expansion requirements. Key considerations include:

(i) **Title and encumbrance check**: Before acquiring or leasing land for a data centre, developers should undertake due diligence to establish the ownership and marketability of title and identify any encumbrances or third-party rights affecting the property. This should include verification of the chain of title, mortgages, charges, easements, rights of way, acquisition notices, pending litigation and competing claims. In addition, the relevant revenue records, mutation entries and existing land-use classification should also be examined to identify any discrepancies in the recorded ownership or status of the land.

(ii) **Government/industrial authority land**: Where the proposed site comprises land allotted or leased by a government or industrial development authority, the allotment or lease terms, transfer restrictions, construction milestones and consequences of non-development should be carefully reviewed to establish the conditions governing the development and operation of the data centre.

(iii) **Land use and conversion:** The existing land use classification of the proposed site and any applicable land-conversion requirements should be assessed at the site-selection stage to determine whether the establishment and operation of a data centre is permitted on the proposed site. Certain state policies exempt or reimburse conversion charges for data centre projects. Some frameworks also allow or facilitate the use/conversion of agricultural land for data-centre development, subject to applicable conditions.

(iv) **Zoning and building norms:** The master or development plan, zoning regulations, building bye-laws and local development regulations applicable to the proposed site should be assessed at the site-selection stage, including requirements relating to floor area ratio (FAR), ground coverage, building height, setbacks and access. In addition, the developer should identify the planning, building, fire-safety, electrical and utility approvals required for the construction and operation of the facility, which vary by state and local authority. Certain state data centre policies provide project-specific relaxations, including enhanced FAR, ground coverage or building-height limits. The availability and applicability of such relaxations should be verified against the relevant state policy and local development regulations. The key approval requirements are set out in *Section VI(B)* below.

(v) **Fibre connectivity:** The site should have access to multiple telecom operators and physically diverse fibre routes, supported by appropriate rights of way.

(vi) **Environmental and coastal zone clearance:** A formal screening should be undertaken at the land-selection stage to determine whether the proposed site or project requires environmental clearance or coastal regulation zone clearance. The applicable

environmental and coastal zone clearance requirements are highlighted in Section *VI(A)(i)* below.

(B) POWER INFRASTRUCTURE

Given the scale and 24×7 operations at a data centre, power availability, reliability and cost are critical to data-centre feasibility. Energy costs account for ~ 65% (sixty-five percent) of a data centre's operating expenditure.[18] Accordingly, the power strategy should consider grid connectivity, renewable power procurement, open-access arrangements, captive generation and backup systems. State policies may offer tariff concessions, electricity exemptions, open-access and captive power arrangements, as discussed in *Section IV(C)* above.

(i) Grid Power

- **Grid availability and capacity:** The developer should assess the availability of adequate grid power for the proposed data centre, including the sanctioned load, available capacity at the nearest suitable substation, transmission capacity, connection voltage, distance from the substation and the infrastructure required to establish the connection.

- **Dedicated infrastructure:** The developer should evaluate the need for dedicated feeders, substations, transformers, and other transmission or distribution infrastructure to establish and maintain a reliable grid connection, including the associated capital expenditure and implementation timelines. Certain state policies provide specific support for such infrastructure. For instance, the Karnataka Data Centre Policy permits dual power connections from two different substations and provides an additional feeder at no cost for data centres with installed capacity above 100 (one hundred) MW.[19]

- **Power redundancy:** In addition to assessing grid availability, developers should also evaluate the availability of independent power supply routes to minimise the risk of outages arising from a failure in any single transmission line or substation. The feasibility of establishing dual-feed connectivity should be evaluated as part of the site power infrastructure design.

(ii) Renewable Energy and Open Access

- **Renewable procurement:** Data centres can meet their power requirements through a combination of renewable energy sources, including solar, wind and hybrid renewable energy arrangements. Such power may be procured through power purchase agreements, captive generation arrangements or open-access procurement, with grid power serving as a supplementary source of electricity to meet residual power requirements.

- **Open access:** The Electricity Act, 2003 and the rules and regulations framed thereunder provide the framework for eligible consumers to procure electricity directly from generators through open access, subject to applicable eligibility conditions, regulatory requirements and charges. Odisha's Data Centre Policy 2022 contemplates facilitating direct procurement from power generators, including renewable-energy generators, subject to the applicable framework.[20]

---

[18] S&P Global, *Will Datacenter Growth in India Propel It to Global Hub Status*, available at: https://www.spglobal.com/en/research-insights/special-reports/india-forward/shifting-horizons/will-data-center-growth-india-propel-country-global-hub-status , accessed on November 18, 2026.

[19] Paragraph 4.3 of Karnataka Data Centre Policy, 2022.

[20] Paragraph 13.1.4 of Odisha State Data Centre Policy, 2022.

- **Captive power:** The Electricity Act, 2003 permits the establishment of captive generating plants and dedicated transmission lines for captive users. Developers considering captive power arrangements should assess the applicable ownership, consumption and other statutory requirements to ensure that the arrangement qualifies as captive generation under the applicable regulatory framework.

(iii) Battery Energy Storage and Backup Power

- **BESS:** Battery Energy Storage Systems ("**BESS**") can support data centre operations by facilitating energy storage, load balancing, renewable-energy integration and backup requirements. Certain state policies recognise BESS as an eligible project component and provide incentives or subsidies for their deployment, subject to prescribed subsidy limits.

- **Conventional backup:** Data centres typically require diesel generator ("**DG**") sets, uninterruptible power supply ("**UPS**") systems, battery banks, automatic transfer systems and emergency electrical systems to maintain continuity during grid interruptions.

- **Diesel infrastructure:** Installation and operation of DG sets and diesel-storage facilities should be assessed against applicable petroleum, environmental and electrical-safety requirements, including requirements arising from the quantity and configuration of fuel storage.

(C) WATER INFRASTRUCTURE

Water availability is an important site-selection consideration for data centres, particularly for large hyperscale and AI-focused facilities where cooling requirements can create significant water demand. While several state policies provide for 24×7 water supply, the adequacy and reliability of the actual supply should be independently assessed. Empirical research indicates that data centres in Greater Noida and Bengaluru operate in areas having groundwater scarcity and may therefore need to consider alternative sources and water-supply arrangements.[21] In Bengaluru, certain facilities have sourced water independently where municipal supply was unavailable,[22] while in Greater Noida, data centres reportedly use freshwater from municipal supply and groundwater.[23]

(i) Water source and availability

The developer should establish the availability and long-term reliability of the proposed water source before committing to a site. Potential sources include municipal/industrial water, treated sewage or wastewater, surface water, groundwater and, where appropriate, desalinated water. Source-specific allocation, extraction and approval requirements should be assessed under the applicable state and local regulatory framework.

---

[21] Down To Earth, *India's Digital Thirst: Data Centres Are Rising in Water-Scarce Regions and Locals Are Paying the Price*, available at: https://www.downtoearth.org.in/science-technology/indias-digital-thirst-data-centres-are-rising-in-water-scarce-regions-and-locals-are-paying-the-price, accessed on September 25, 2026.

[22] Down To Earth, *India's Digital Thirst: How Bengaluru's Tech Dreams Are Colliding with a Worsening Water Crisis*, available at: https://www.downtoearth.org.in/science-technology/indias-digital-thirst-how-bengalurus-tech-dreams-are-colliding-with-a-worsening-water-crisis, accessed on September 25, 2026.

[23] Down To Earth, *India's Digital Thirst: A Booming Data Centre Corridor in Uttar Pradesh's GB Nagar is Running on Empty Wells*, available at: https://www.downtoearth.org.in/water/indias-digital-thirst-a-booming-data-centre-corridor-in-uttar-pradeshs-gb-nagar-is-running-on-empty-wells, accessed on September 25, 2026.

For example, in Gautam Buddha Nagar, Uttar Pradesh, groundwater extraction is subject to district-level regulation and groundwater users may be required to undertake groundwater recharge at a ratio of 2 (two) litres recharged for every 1 (one) litre extracted along with rainwater-harvesting measures. For a large facility, the developer should factor any source-specific extraction limits and restrictions into the site's water-management plan at the outset.

(ii) Groundwater

Groundwater may be considered as a potential water source subject to the applicable regulatory framework and site-specific groundwater conditions. Depending on the location and groundwater status, extraction may require approval or a no-objection certificate ("**NOC**") from the Central Ground Water Authority ("**CGWA**") or the relevant state authority. As part of due diligence, the developer should assess the permissibility of groundwater extraction, the applicable groundwater classification and availability, the permitted extraction quantity and recharge obligations.

(iii) Cooling technology and water efficiency

Water requirements should be assessed together with the proposed cooling architecture. Cooling towers and evaporative systems may consume significant water, while air-cooled and dry-cooling systems can reduce direct water consumption, potentially at the cost of higher energy usage. Closed-loop systems may also reduce water consumption, depending on their design and operating conditions. Some data centres in India, in their goal towards sustainability, are adopting air-cooled chillers with high water temperature and cooling accessories to maintain optimal environmental conditions. Accordingly, the developer should assess water usage effectiveness alongside power usage effectiveness to evaluate the trade-off between water consumption and energy efficiency.

(iv) Recycled water and treatment infrastructure

Where technically and economically feasible, data centres should prioritise treated wastewater and non-potable water sources for cooling and other non-domestic requirements to reduce dependence on freshwater. Potential sources include treated municipal sewage, recycled wastewater and industrial treated water. The developer should also assess the quality of water available for cooling and the treatment infrastructure required to meet the specifications of the proposed cooling system.

State policies may provide incentives for water-management infrastructure. For example, Rajasthan provides incentives relating to wastewater treatment, water infrastructure and rainwater harvesting. Developers and investors should therefore assess the availability of such incentives when evaluating the overall water infrastructure requirements and operating costs of a proposed facility.

VI. REGULATORY AND PERMITS FRAMEWORK

Setting up a data centre in India requires approvals, licences, consents, clearances and NOCs from central, state and local authorities, depending on the project's location, design and operations. The regulatory framework spans environmental protection, pollution control, water and groundwater management, waste management, building construction, fire safety, electrical infrastructure, power procurement, labour law, cybersecurity and data protection. Several Indian states have introduced single-window clearance mechanisms to streamline and expedite approval processes. This section provides a high-level overview of the key approvals and compliance requirements relevant to the establishment and operation of a data centre in India.

(A) ENVIRONMENTAL CLEARANCE

(i) The Environment (Protection) Act, 1986

The Environment (Protection) Act, 1986 is the umbrella legislation under which the key environmental rules and notifications applicable to data centres are framed, including the Environmental Impact Assessment Notification, 2006 ("**EIA Notification**"), the Coastal Regulation Zone Notification, 2019 ("**CRZ Notification**") and the various waste management rules.

- EIA Notification: Under the EIA Notification, a data centre is not independently listed as a project category requiring mandatory environmental clearance. However, prior environmental clearance may be required from the state environment impact assessment authority where the project's built-up area exceeds (twenty thousand) square metres (as a building and construction project) or where the campus exceeds 50 (fifty) hectares or 1,50,000 (one hundred fifty thousand) square metres of built-up area (as an area development project). The relevant thresholds, project classification and competent authority should be assessed against the EIA Notification before construction.

- CRZ Notification: Where a proposed data centre is proposed to be located in a coastal state or a union territory and the site or proposed development falls within the Coastal Regulation Zone ("**CRZ**"), prior CRZ clearance is required for activities regulated or permitted under the CRZ Notification before commencement of the relevant development activity. The applicable CRZ and corresponding restrictions depend on the CRZ Notification and the approved coastal zone management plan. The CRZ Notification classifies coastal areas into CRZ-I, CRZ-II, CRZ-III and CRZ-IV, with different restrictions and permissible activities depending on the nature and location of the area. A prior approval must be taken from the state coastal zone management authority or Ministry of Environment, Forest, and Climate Change, as applicable, before any development is undertaken. Accordingly, the proposed data-centre site should be screened against the coastal zone management plan, including the demarcation of the HTL and applicable CRZ category, at the site-selection and project-planning stage.

(ii) Pollution control consents

The establishment and operation of a data centre is subject to the consent regime administered by the relevant State Pollution Control Board ("**SPCB**") or Pollution Control Committee ("**PCC**") under the Water (Prevention and Control of Pollution) Act, 1974 and the Air (Prevention and Control of Pollution) Act, 1981. Data centres falling within the applicable consent regime are generally required to obtain a consent to establish ("**CTE**") prior to establishment and a consent to operate ("**CTO**") prior to commencement of operations. The applicable consents may prescribe conditions relating to wastewater generation, treatment and discharge as well as air emissions from DG sets and associated monitoring and pollution-control measures. Data centres must also comply with applicable DG-set emission standards and the Noise Pollution (Regulation and Control) Rules, 2000.

(iii) Groundwater Extraction NOC

For data centres to use groundwater for cooling or other operational requirements, an NOC is required from CGWA or the relevant state groundwater authority, depending on the applicable jurisdiction and regulatory framework. The CGWA framework also provides for groundwater abstraction charges, water-flow meters, extraction monitoring and reporting, rainwater harvesting, recharge measures and water audits, wherever

applicable. Accordingly, availability of an adequate and legally permissible water source, groundwater categorisation and the feasibility of recycled-water and rainwater-recharge systems should be assessed at the site-selection and design stage.

(iv) Waste Management

Data centres generate different categories of regulated waste, which are governed by separate waste-management rules prescribed under the Environment (Protection) Act, 1986. Waste must be segregated and channelised in accordance with the applicable waste-specific rules.

- Hazardous waste: The Hazardous and Other Wastes (Management and Transboundary Movement) Rules, 2016 apply to hazardous and other wastes generated from data-centre operations, including used/spent oil and other wastes falling within the categories specified under the rules. Where applicable, the occupier is required to obtain authorisation from the concerned SPCB/PCC and comply with the prescribed storage, handling, record-keeping and disposal requirements.

- E-waste: The E-Waste Management Rules, 2022 govern the management and environmentally sound disposal of electronic waste generated from electrical and electronic equipment. Data centres should ensure that end-of-life servers, networking equipment and other covered IT hardware are channelised through the prescribed authorised or registered entities.

- Waste batteries: The Battery Waste Management Rules, 2022 regulate the collection, recycling and disposal of waste batteries. Data centres deploying large-scale battery banks for uninterruptible power supply and backup power systems should ensure channelisation of spent batteries through registered entities and comply with record-keeping requirements.

- Solid waste: The Solid Waste Management Rules, 2026 regulate the management of solid waste generated from commercial and other non-residential establishments. Data centres must comply with applicable source-segregation, collection, storage, processing and disposal requirements. A data centre may also qualify as a 'Bulk Waste Generator' where it meets any of the prescribed thresholds, including a floor area of 20,000 (twenty thousand) sq. m. or more, water consumption of 40,000 (forty thousand) litres or more per day, or generation of 100 (one hundred) kg or more of solid waste per day, in which case additional obligations under the rules would apply.

(B) BUILDING AND INFRASTRUCTURE APPROVALS

In the context of land and building, the development of a data centre typically requires a combination of land-use, planning, building, fire-safety, electrical and utility approvals, with the specific approvals and competent authorities varying by state, local planning authority and the characteristics of the project. Accordingly, the applicable master/development plan, zoning regulations, building bye-laws and local development regulations should be reviewed at the site-selection stage.

(i) Land Use and Building Approvals

The proposed site must permit the intended data-centre use under the applicable master plan, zoning regulations or development plan. Depending on the jurisdiction, data centres may fall within IT/ITeS, commercial, industrial or other permitted-use categories.

Building and site plans must be approved by the competent local or planning authority under the applicable state and local building and development regulations. The National Building Code of India, 2016 ("**NBC**") provides a national model framework for development control and building requirements. Its binding application depends on adoption or incorporation into the relevant legal framework. For example, the Tamil Nadu Combined Development and Building Rules, 2019 provide the regulatory framework for development and building approvals in Tamil Nadu and require compliance with the applicable provisions of the NBC.

The review may cover applicable requirements relating to FAR, ground coverage, height, setbacks, access, parking, structural safety, fire safety and other development controls, subject to relaxations provided under the data centre policies by the states. Requirements for large or specialised installations such as substations, transformers, DG sets, cooling equipment and rooftop installations should also be assessed under the applicable local regulations.

Depending on the state and local framework, a commencement/building permit or equivalent approval may be required before construction, followed by a completion certificate and/or occupancy certificate before occupation or use of the building.

(ii) Fire and Life Safety

Fire-safety compliance is governed by the applicable state legislation, rules and local building regulations, read with relevant NBC provisions. For example, in Uttar Pradesh, the Uttar Pradesh Fire and Emergency Services Act, 2022 provides the statutory framework for fire prevention and fire safety. Depending on the jurisdiction and project, a fire NOC or other approval may be required at the design, construction or occupancy stage. Requirements may cover access and egress, fire-resistant construction, detection and alarm systems, suppression systems, emergency exits and fire-fighting water infrastructure.

(iii) Electrical Infrastructure

Data-centre electrical installations must comply with the Electricity Act, 2003, the Central Electricity Authority (Measures relating to Safety and Electric Supply) Regulations, 2023 ("**CEA Regulations**"), and applicable State electrical-safety requirements. The applicable inspection, self-certification and approval process should be determined by reference to the installation and relevant regulatory thresholds. Requirements should be assessed for substations, transformers, generating units and other electrical infrastructure.

(iv) DG Sets and Fuel Storage

DG sets are subject to applicable emission, noise, electrical-safety and fire-safety requirements and relevant SPCB/PCC conditions. On-site storage of diesel or other petroleum products must be assessed under the Petroleum Act, 1934, the Petroleum Rules, 2002 and applicable fire-safety requirements. Any PESO approval or licence should be determined by reference to the type, quantity and configuration of the proposed storage.

(v) Power and Energy Approvals

The Electricity Act, 2003 provides the overarching framework for electricity generation, transmission, distribution and open access. A data centre may obtain power through conventional grid supply, open access, captive generation, renewable-energy arrangements or a combination of these, subject to applicable DISCOM,

transmission/distribution utility, and grid-connectivity requirements. The act permits a person to establish and operate a captive generating plant and dedicated transmission lines, subject to the statutory requirements and applicable regulations.

Further, the Electricity (Promoting Renewable Energy Through Green Energy Open Access) Rules, 2022 facilitate procurement of renewable electricity through green open access. Developers should therefore assess green open access eligibility, connectivity, transmission/wheeling charges, cross-subsidy and additional surcharges.

(C) DATA PROTECTION, CYBERSECURITY AND DATA LOCALISATION

(i) Data Protection Framework

Data-centre operators must assess data-protection obligations by reference to the services provided and their role in processing personal data. The Information Technology Act, 2000 ("**IT Act**") and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("**SPDI Rules**") govern the protection of sensitive personal data, including requirements relating to privacy policies and reasonable security practices. The Digital Personal Data Protection Act, 2023 ("**DPDP Act**") and the Digital Personal Data Protection Rules, 2025 ("**DPDP Rules**") establish the future framework for processing digital personal data, including requirements relating to notice and consent, security safeguards, breach management, data-subject rights and accountability of Data Fiduciaries and Data Processors.

The classification of a data-centre operator as a Data Fiduciary[24] or Data Processor[25] depends on whether it determines the purpose and means of processing or merely processes data on its customer's documented instructions. In a data centre service arrangement, the data centre service provider would generally be construed as a Data Processor, while the customer of the data centre would generally be the Data Fiduciary, where the customer determines the purpose and means of processing the personal data. Typically, such customers may include corporates or institutions operating in the banking, financial services and insurance sectors, technology companies, e-commerce companies and other businesses that, *inter alia*, process personal data on a large scale. Where the data centre operator itself determines the purpose and means of processing personal data for its own business purposes, it may instead be the Data Fiduciary in respect of such processing.

The substantive DPDP provisions will be enforceable from May 13, 2027, and upon commencement of the substantive provisions, Section 43A of the IT Act and the SPDI Rules will be repealed.

(ii) Data Localisation and Cross-Border Transfers

The DPDP Act does not provide for a blanket India-only storage requirement for personal data. Cross-border transfers are generally permitted subject to countries/territories that may be restricted by the Central Government and any stricter requirements under other Indian laws. Additional requirements may apply to Significant Data Fiduciaries,[26] including restrictions concerning specified personal data and traffic data under the DPDP Rules.

---

[24] Under the DPDP Act, Data Fiduciary means any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data.

[25] Under the DPDP Act, Data Processor means any person who processes data on behalf of the Data Fiduciary.

[26] Under the DPDP Act, Significant Data Fiduciaries means any data fiduciaries or classes of data fiduciaries notified as such by the Central Government having regard to factors including the volume and sensitivity of personal data processed, risk to the rights of data principals and potential impact on the sovereignty and integrity of India, security of the State, electoral democracy and public order.

(iii) Sector-Specific Localisation

Other than the requirements provided under the IT Act, DPDP Act, and DPDP Rules, separate data-localisation requirements may apply to particular types of data. For instance, the Reserve Bank of India requires payment-system data to be stored in India. Similar sector-specific requirements may apply to banking/financial services, insurance, securities, telecommunications and government/critical infrastructure data, depending on the nature of the customer and the applicable regulator. Another example is the Insurance Regulatory and Development Authority of India's framework, which provides requirements concerning the maintenance and location of insurance records and data within India.

(iv) Cybersecurity and Critical Infrastructure

The directions issued by the Indian Computer Emergency Response Team ("**CERT-In**") relating to information security practices, procedure, prevention, response and reporting of cyber incidents for safe & trusted Internet ("**CERT-In Directions**") apply to covered entities and prescribe cybersecurity incident reporting and related obligations. These include reporting specified cyber incidents within six hours of noticing them or being informed of them, securely maintaining information and communication technology ("**ICT**") system logs for 180 (one hundred eighty) days within Indian jurisdiction, and synchronising system clocks with designated time source. Data-centre and cloud service providers must also assess the specific customer-information and information-production requirements applicable to them.

(D) LABOUR LAW COMPLIANCES

Data-centre operations are generally less labour-intensive, with the core operational workforce typically comprising IT, engineering, security and facility-management personnel. However, labour-law compliance remains relevant both to the direct workforce and to contract labour engaged for security, housekeeping, maintenance and other services. The applicability of particular labour and employment requirements will depend, amongst other things, on the number and category of workers, the nature of activities and the engagement structure.

The four Labour Codes, i.e. the Code on Wages, 2019, Industrial Relations Code, 2020, Code on Social Security, 2020, and Occupational Safety, Health and Working Conditions Code, 2020, came into force on November 21, 2025, consolidating the erstwhile 29 (twenty-nine) central labour laws. Their implementation is supplemented by rules and state-level requirements.

While the Labour Codes have come into force, the procedural framework for their implementation is dependent on the rules prescribed by the appropriate government. As the appropriate government for several provisions applicable to private establishments is the state government, the relevant state rules are required to operationalise various procedural and administrative requirements, including prescribed forms, registers, records and other compliances. Pending notification of the applicable state rules, the substantive provisions of the Labour Codes that have come into force should be complied with, to the extent applicable. With respect to the procedural requirements, the rules framed under the corresponding erstwhile enactments may continue to be followed until the applicable Labour Code rules are notified.

(i) Wages and Employment Conditions

The Code on Wages, 2019 regulates minimum wages, payment of wages, deductions, bonus and non-discrimination in wages. Data centre operators must also comply with applicable requirements concerning appointment letters, working hours, overtime,

leave, holidays and maintenance of employment records, as prescribed under the applicable framework.

(ii) Social Security and Employee Benefits

The Code on Social Security, 2020 governs applicable provident fund, employee state insurance, gratuity, maternity benefits, employees' compensation and other social-security obligations, subject to the relevant coverage and thresholds. Data-centre operators should assess these requirements for both their direct workforce and eligible categories of workers engaged through contractors. The code also expands the statutory framework to cover unorganised, gig and platform workers where the relevant provisions/schemes apply.

(iii) Occupational Safety, Contract Labour and Construction Workforce

The Occupational Safety, Health and Working Conditions Code, 2020 ("**OSH Code**") is particularly relevant to data-centre projects because of the presence of electrical infrastructure, DG sets, fuel storage, mechanical and cooling equipment and other potentially hazardous operations. It addresses occupational safety and health, working conditions, welfare facilities for workers, contract labour and inter-state migrant workers, with applicability depending on the establishment, workforce and nature of activities.

(iv) State Labour Laws and Contractor Compliance

In addition to the Labour Codes, data centres must comply with state-specific labour requirements, including applicable shops and establishments legislation and state rules framed under the Labour Codes. Shops and establishments legislation typically regulates conditions of employment in commercial establishments, including working hours, leave, holidays, overtime, maintenance of registers and records, and other employer obligations. Depending on the location and nature of the data-centre operations, registration and other compliance requirements under the applicable state shops and establishments legislation may also apply.

VII. CONCLUSION

India's data-centre sector is entering a phase of significant expansion, supported by the growth of AI, cloud computing and digital consumption, increasing investment by global and domestic operators, and growing policy support. The expansion of the sector is also creating opportunities across data-centre development, power and renewable-energy infrastructure, cooling, connectivity and related digital infrastructure.

For investors, the opportunity extends beyond the growth in data-centre capacity itself. The availability of dedicated state incentives, improving infrastructure and the emergence of new data-centre markets create opportunities to structure projects around location-specific advantages and long-term operating economics. Power and water availability, connectivity, regulatory approvals and compliance remain important considerations. The associated risks can be mitigated through appropriate site selection, early regulatory planning and project structuring.

Contributed by:



Saurav Kumar
Senior Partner



Swathi Sreenath
Partner



Shreya Chaturvedi
Principal Associate



Kaustubh Garg
Associate

DISCLAIMER

This document is merely intended as an update and is merely for informational purposes. This document should not be construed as a legal opinion. No person should rely on the contents of this document without first obtaining advice from a qualified professional person. This document is contributed on the understanding that the Firm, its employees and consultants are not responsible for the results of any actions taken on the basis of information in this document, or for any error in or omission from this document. Further, the Firm, its employees and consultants, expressly disclaim all and any liability and responsibility to any person who reads this document in respect of anything, and of the consequences of anything, done or omitted to be done by such person in reliance, whether wholly or partially, upon the whole or any part of the content of this document. Without limiting the generality of the above, no author, consultant or the Firm shall have any responsibility for any act or omission of any other author, consultant or the Firm. This document does not and is not intended to constitute solicitation, invitation, advertisement or inducement of any sort whatsoever from us or any of our members to solicit any work, in any manner, whether directly or indirectly.

You can send us your comments at:

knowledgecentre@argus-p.com

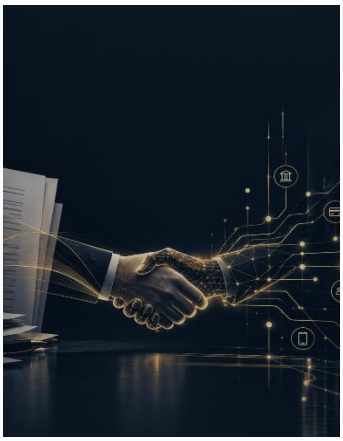
Mumbai I Delhi I Bengaluru I Kolkata

www.argus-p.com

Recent Papers/ Articles



September 2026
Emissions Trading and Carbon Credits in India: A Legal Perspective
Energy and Infrastructure



August 2026
When does settlement become a payment system?
Corporate and M&A; Finance



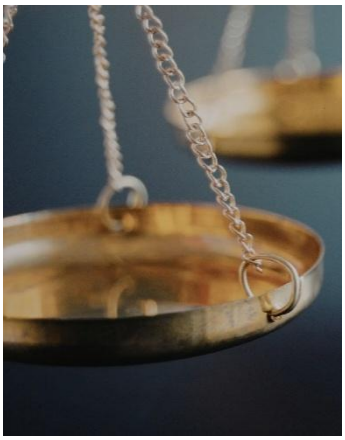
September 2026
Revision to EPF Wage Ceiling: Coverage, Contributions and the September Transition
Labour & Employment



August 2026
A New Era for Real Estate Insolvency: IBC (Amendment Act) 2026 and the IBBI Discussion Paper
Corporate Restructuring & Insolvency



June 2026
Cracking the Code II: The New Central Labour Rules at a Glance
Labour and Employment



May 2026
Sophie's Choice: The Entitlement of Dissenting Financial Creditors
Corporate Restructuring & Insolvency

For more Papers/ Articles click here.



MUMBAI
11, Free Press House
215, Nariman Point
Mumbai 400021
T: +91 22 67362222

DELHI
7A, 7th Floor, Tower C,
Max House,
Okhla Industrial Area, Phase 3,
New Delhi 110020
T: +91 11 69044200

KOLKATA
Binoy Bhavan
3rd Floor, 27B Camac Street
Kolkata 700016
T: +91 33 40650155/56

BENGALURU
20th Floor, SKAV 909,
Lavelle Road
Bengaluru – 560001
T: +91 80 46462300

www.argus-p.com I communications@argus-p.com