KING STUBB & KASIVA
ADVOCATES AND ATTORNEYS

INDIA DATA CENTER REPORT

2026

Legal, Regulatory & Investment Landscape

Technology, Media & Telecommunications · Data Privacy ·

March 2026 . Confidential . For Client Use Only

Important Notice

This report has been prepared by King Stubb & Kasiva, Advocates and Attorneys ("KSK") exclusively for informational purposes. Nothing contained herein constitutes legal advice, and no attorney-client relationship is created by reason of its receipt or use. The analysis reflects the state of law, regulation, and market intelligence available as of March 2026. Laws, regulations, and market conditions are subject to change, and KSK accepts no responsibility for decisions taken in reliance on this report without obtaining specific legal counsel.

About King Stubb & Kasiva

King Stubb & Kasiva ("KSK") is a full-service national law firm in India with offices in New Delhi, Mumbai, Bengaluru, Chennai, Hyderabad, Kochi & Pune. KSK has alliances with associate lawyers in all states and union territories of India and international locations. We can cater to all corporate legal, regulatory and dispute resolution requirements of our clients across the length and breadth of the country. We also have a huge informal network of international law firms across ninety-seven countries.

We represent large, medium & small business houses, multinational corporations, banking & financial institutions, technology and manufacturing pioneers, private equity and venture capital investors and start-ups across the country.

KSK does not just provide legal expertise; we take a position and provide commercially savvy advice – we partner with our clients to deliver the best business solutions. We do this by knowing their industries, the trends and issues, and their competitors. We are always focused on providing interactions between our firm and our client which delivers the highest levels of integrity, hard work and trust in order to create a perfectly professional relationship.

The prime motive revolving around any business is to reduce expenditure and increase revenue. We collaborate with the client to highlight legal risks and advise steps and solutions to mitigate these to achieve the business objectives.

At KSK, we have established a client-oriented team to ensure that our services meet the most exacting standards. All clients have constant support from their contact at the firm at any time, day, or night, for routine legal matters or intricate issues requiring creative problem-solving.

KSK's proactive way provides value to our clients by looking ahead towards unforeseen issues, articulating them, and mapping out a service plan for their future needs.

Contents

I. Executive Summary

India's data center market was valued at approximately USD 8.94 billion as of 2025 and is projected to reach USD 31.36 billion by 2035. Operational capacity reached 1,520 megawatts by the close of 2025, with a further 3,930 MW under construction or in advanced development, placing total installed capacity on a trajectory toward 5,450 MW by end-2026. Cumulative foreign direct investment into the sector exceeded USD 14.7 billion between 2020 and April 2025, with Microsoft and Google alone committing in excess of USD 30 billion in India-wide cloud and infrastructure investment.

From a legal and regulatory standpoint, 2025 and 2026 represent the most consequential period in the history of India's data governance architecture. The notification of the Digital Personal Data Protection Rules on 13 November 2025 triggered an 18-month compliance runway - concluding on 13 May 2027 - within which every significant data center operator, cloud service provider, and enterprise occupier must achieve full compliance with India's comprehensive data protection framework. Penalties for non-compliance extend to INR 250 crore (approximately USD 30 million) per breach. Simultaneously, sector-specific localisation mandates from the Reserve Bank of India, the Securities and Exchange Board of India, and the Insurance Regulatory and Development Authority of India continue to operate independently, creating compulsory domestic infrastructure demand estimated at 1,200 MW by 2027.

This report, prepared by KSK's Technology, Media & Telecommunications practice, provides a comprehensive analysis of the legal, regulatory, contractual, and transactional landscape for data centers in India. It is intended to serve as a primary reference document for institutional investors evaluating the sector, operators structuring market entry, enterprise occupiers managing compliance obligations, and financial institutions providing capital to the industry.

India's data center investment story is distinguished from comparable emerging market opportunities by the simultaneity and scale of its demand catalysts. The convergence of DPDP compliance obligations, sectoral localisation mandates, AI infrastructure investment, and hyperscaler cloud region commitments within a compressed 24-month window creates a demand environment that no single catalyst could replicate. Investors and operators who position infrastructure capital ahead of the May 2027 compliance deadline are best placed to capture the premium colocation pricing and pre-lease commitments that will characterise the market through 2028.

II. Market Overview and Growth Trajectory

2.1 Market Sizing and Projections

India's data center market has demonstrated sustained compound growth over the preceding five years, accelerating materially from 2023 onward as hyperscale commitments translated into capital deployment. The market was valued at USD 3.40 billion in 2023, USD 5.03 billion in 2024, and is estimated at USD 8.94 billion in 2025 - representing 78% year-on-year growth in the most recent completed year. Multiple independent analysts project market scale of USD 22–31 billion by the middle of the next decade, with projected CAGRs ranging from 13.37% (Mordor Intelligence) to 22.79% (Astute Analytica) depending on scope of measurement.

Table1: *India Data Center Market - Revenue and Growth Projections*

Year	Market Size (USD Bn)	YoY Growth	Principal Catalyst
2021	1.20	—	Post-pandemic digitalisation; initial cloud migration
2022	2.10	+75%	Cloud adoption acceleration; 5G spectrum auctions
2023	3.40	+62%	Hyperscale market entry; infrastructure status grant
2024	5.03	+48%	AI workload demand; submarine cable commissioning
2025	8.94	+78%	DPDP Rules notification; Google-Adani alliance; NTT expansion
2026E	10.70	+20%	Compliance-driven demand; 5,450 MW installed milestone
2028E	14.50	+16%	Green data center mandates; edge compute buildout
2031E	22.00	+15%	15,210 MW projected capacity; full DPDP regime operational
2035E	31.36	+10%	Market maturity; India established as global Tier I hub

Source: Mordor Intelligence; Astute Analytica; Arizton Advisory; Grand View Research. KSK Analysis, March 2026.

2.2 Installed Capacity and Geographic Distribution

Operational capacity reached approximately1,520 MW across India by the close of 2025, representing a net addition of 387 MW within a single calendar year - more than double the 191 MW added in 2024. On an installed basis - inclusive of capacity under active construction - the market is estimated at 4,480 MW in 2025, rising to approximately 5,450 MW by end-2026. JLL projects that India will reach 15,210 MW of total capacity by 2031, placing it among the top five global data center markets by that date.

Geographic concentration remains pronounced. Mumbai and Navi Mumbai account for approximately 52% of national operational capacity (approximately 790 MW), driven by the city's status as India's primary financial centre, its position as the landing point for the largest number of submarine cables

and the concentration of BFSI-sector colocation demand. Chennai has emerged as the most significant challenger hub, with approximately 305 MW operational, benefiting from lower land and power costs, direct connectivity to Southeast Asian submarine cable systems, and state government support under Tamil Nadu's active data center policy.

Table 2: *Geographic Distribution of Operational Data Center Capacity (2025)*

Hub	Operational MW	Share	Key Competitive Characteristic
Mumbai / Navi Mumbai	790	52%	BFSI colocation; submarine cable proximity; Tier I financial centre
Chennai	305	20%	Power cost advantage; SE Asia cable connectivity; Tamil Nadu policy
Bengaluru	182	12%	Technology sector demand; AI workloads; Karnataka renewable tariffs
Hyderabad	152	10%	Pharmaceutical and tech sector; HITECH City; Telangana incentives
Delhi-NCR / Noida	76	5%	Government and PSU demand; YEIDA corridor; UP data center policy
Other (Pune, Kolkata)	15	1%	Emerging markets; enterprise proximity requirements

Source: JLL India Data Center Report Q4 2025; Savills India Research. KSK Analysis.

2.3 Principal Demand Drivers

India's data center demand is underpinned by a convergence of structural, regulatory, and technology forces that distinguish the market from other high-growth geographies. Unlike demand cycles driven by a single catalyst, the Indian market benefits from at least six independent and mutually reinforcing demand vectors, each of which would, on a standalone basis, justify meaningful capacity investment.

Digital Public Infrastructure and Government Digitalisation. The Indian government's Digital Public Infrastructure stack comprising Aadhaar (biometric identity), UPI (payments), DigiLocker (document storage), and ONDC (open commerce) collectively processes in excess of 14 billion transactions per month and generates sustained, non-discretionary demand for sovereign and near-sovereign compute infrastructure. The GI Cloud (Meghraj) programme mandates that all government data reside on NIC-managed or approved domestic cloud infrastructure, creating a captive demand base that is structurally insulated from private sector investment cycles. The National Data Governance Framework, currently in final consultation, is expected to further concentrate government workloads on domestic infrastructure and expand the mandatory domestic cloud footprint.

Artificial Intelligence and GPU Workload Expansion. The proliferation of large language model training, inferencing, and AI-powered enterprise applications is generating demand for high-density compute infrastructure that is materially different in power and cooling profile from conventional IT workloads. AI-optimised racks typically require 30–100 kW of power per rack unit, compared to 5–15 kW for standard IT infrastructure, requiring investment in direct liquid cooling, high-performance interconnect fabric, and purpose-built power distribution. India's combination of a large domestic AI developer community, significant sovereign AI investment (including the government's USD 1.16 billion AI infrastructure commitment and NVIDIA's partnership with Reliance Industries), and competitive colocation pricing relative to the United States and Singapore positions the country as an increasingly credible destination for GPU cluster deployments.

III. Legal and Regulatory Framework

3.1 The Digital Personal Data Protection Framework

The DPDP Rules simultaneously established the Data Protection Board of India as the primary enforcement authority and triggered a phased compliance timeline. Rules 1, 2, and 17–21 took effect immediately upon notification. Rule 4, governing the registration and operation of Consent Managers, becomes effective on 13 November 2026. All remaining substantive obligations - including the appointment of Data Protection Officers, implementation of security safeguards, breach notification obligations, Data Principal rights infrastructure, and children's data protections - become enforceable on 13 May 2027. The Board is empowered to impose financial penalties of up to INR 250 crore (approximately USD 30 million) per contravention.

KSK Legal Alert - DPDP Compliance Timeline
13November 2025:Data Protection Board of India constituted; Rules 1, 2 and 17–21 operative. 13 November 2026: Consent Manager framework (Rule 4) operative. 13 May 2027: All substantive Data Fiduciary obligations enforceable - security safeguards (Rule 6), breach notification (Rule 7), data retention limits (Rule 8), Data Principal rights mechanisms (Rule 14), children's data obligations (Rules 10–12), and Significant Data Fiduciary requirements (Rule 13) including annual Data Protection Impact Assessments and algorithmic audits. KSK strongly advises against waiting for the 2027 deadline: programme offices, gap assessments, and vendor contract reviews require 18–24 months of sustained effort and should commence immediately.

On data localisation, the DPDP Act adopts a liberal default position by international standards. Cross-border personal data transfers are permitted by default, subject to the Central Government's power to notify jurisdictions or classes of data to which transfers are restricted - a so-called 'blacklist' model. Rule 15 grants the Government broad discretion to impose restrictions. Market participants should note that this liberal default is subject to revision and that sectoral localisation mandates - which are entirely independent of the DPDP framework - continue to impose hard residency requirements in several critical industries.

3.2 Sectoral Data Localisation Mandates

India's sector-specific localisation obligations predate the DPDP Act and operate independently of it. They are immediately operative, subject to no grace period, and carry regulatory sanctions ranging from monetary penalties to licence revocation. For data center operators and enterprise occupiers in regulated industries, these obligations are more immediately material than the DPDP framework and must be addressed with corresponding urgency.

Table 3: *Sectoral Data Localisation Mandates — India*

Sector	Regulator	Localisation Requirement	Sanction
Payment Systems	Reserve Bank of India	All payment system data must be stored exclusively in India. Master Direction on Storage of Payment System Data, 2018.	Regulatory action; payment system licence revocation.
Securities Markets	SEBI	All regulated entity data to reside only in India. SEBI Circular on Cloud Framework for Regulated Entities, 2023.	Regulatory direction; penalty under SEBI Act.
Insurance	IRDAI	Policy records, claims data and other insurance data must be stored in India. IRDAI Circular on Data Localisation, 2015.	Regulatory sanction; potential licence cancellation.
Telecommunications	DoT / TRAI	Traffic data and subscriber records subject to India-residence obligations under telecom licensing conditions.	Licence condition breach; financial penalty.
Government / Public	MeitY / NIC	All government data on NIC infrastructure or approved domestic cloud under GI Cloud (Meghraj) policy.	Contract termination; debarment from government contracts.
Healthcare (Proposed)	Digital Health Authority	Electronic health records under ABDM framework; formal mandate anticipated in 2026.	Anticipated regulatory direction pending formal notification.

Source: RBI Master Direction 2018; SEBI Cloud Framework Circular 2023; IRDAI Circular 2015; DoT Licensing Conditions; MeitY GI Cloud Policy.

3.3 Infrastructure Status and Policy Incentives

State governments have competed aggressively for data center investment by supplementing central infrastructure status with state-level incentive packages. Maharashtra offers a 25% stamp duty exemption on land purchases, a power tariff subsidy of INR 2 per kWh, and single-window clearance. Tamil Nadu provides 100% reimbursement of State GST for five years and a 3% interest subvention on capital expenditure loans. Andhra Pradesh's Data Center Policy 4.0 targets 200 MW of additional capacity with land allotment and fiscal support. Karnataka offers access to among the lowest renewable power tariffs in India (INR 2.90–3.40 per kWh).

3.4 Cybersecurity and Critical Information Infrastructure

The Information Technology (Amendment) Act, 2008 and the rules promulgated thereunder vest CERT-In (the Indian Computer Emergency Response Team) with authority over cybersecurity incident reporting. CERT-In Direction 2022 imposes a mandatory six-hour reporting obligation for cybersecurity incidents affecting critical sectors - including financial services, healthcare, energy, and government - and requires data centers serving such clients to maintain technical infrastructure capable of detecting and reporting incidents within this window.

The CII designation framework under Section 70 of the IT Act is of particular relevance to large-scale data center operators. The Government has the authority to designate any computer resource as Critical Information Infrastructure, the effect of which is to impose enhanced security obligations, mandatory access control protocols, and incident coordination requirements with CERT-In. Operators whose facilities host financial services, healthcare, energy, or government workloads should assess their CII designation exposure proactively, as designation triggers an immediate compliance uplift that may require capital investment in technical security infrastructure.

Practical Compliance Posture

Data center operators serving clients in regulated sectors should maintain: a dedicated CERT-In-compliant Security Operations Centre (SOC) with 24x7 monitoring capability and a documented six-hour incident detection and reporting workflow; network segmentation that isolates critical client workloads from general IT infrastructure; regular penetration testing (minimum annually for CII-adjacent facilities); and a practised incident response playbook that includes regulatory notification procedures to both CERT-In and affected Data Fiduciaries. KSK advises that these technical requirements be explicitly addressed in master service agreements and colocation contracts, with the operator providing quarterly compliance attestations to regulated entity clients.

Operators should also be aware of CERT-In's power to audit data center facilities directly in connection with cybersecurity incidents or CII designation reviews. CERT-In audits have become more frequent since the 2022 Direction, and operators without documented security programmes, incident response procedures, and SOC logs covering a minimum 180-day rolling period have faced regulatory notices. KSK advises that data center operators retain specialist cybersecurity counsel to conduct a CERT-In readiness audit on an annual basis and address identified gaps before they become the subject of regulatory enquiry.

IV. Investment Landscape and Major Transactions

4.1 Capital Flows

India attracted approximately USD 14.7 billion in cumulative data center investment between 2020 and April 2025. Foreign institutional investors accounted for approximately 86% of total inflows, reflecting the global capital markets' confidence in India as a sovereign data center jurisdiction. The committed pipeline through 2026 is estimated at a further USD 5.7 billion in deployed or near-deployed capital, with analysts projecting USD 20–25 billion in additional investment through 2030. The sector's investment profile has shifted meaningfully toward long-duration commitments: hyperscaler announcements from Microsoft (USD 3 billion), Google (USD 15 billion alliance with Adani), and Amazon Web Services signal a decadal commitment to Indian digital infrastructure rather than a cyclical investment wave.

4.2 Landmark Transactions (2024–2026)

The following transactions represent the most commercially and legally significant events in the Indian data center market in the relevant period. KSK's commentary identifies the principal legal structuring considerations arising from each transaction.

Table 4: *Landmark Data Center Transactions — India (2024–2026)*

Date	Transaction	Value	Legal Structuring Note
Oct 2025	Google and Adani Group strategic alliance for cloud regions in Bengaluru, Delhi-NCR, and Mumbai. First 80 MW site scheduled for commissioning mid-2026.	USD 15B	JV structuring; CCI clearance; long-term grid supply agreements; FEMA compliance on FDI structure.
Dec 2025	AdaniConneX commissions 400 MW Chennai campus with 200 MW integrated renewable energy supply. Tier IV certification achieved.	Undisclosed	PPA structuring; Renewable Energy Certificate compliance; EPC contract negotiation.
Nov 2025	Yotta Infrastructure completes USD 200M debt raise for 250 MW Greater Noida project with 100 MW solar and 50 MW battery storage.	USD 200M	External Commercial Borrowing documentation; security package; REC procurement.
Nov 2024	Colt DCS and RMZ Corp establish USD 1.7B joint venture targeting hyperscale demand across Mumbai and Bengaluru AI-driven infrastructure campuses.	USD 1.7B	JV shareholder agreement; FEMA inbound investment structuring; hyperscale pre-lease documentation.
Jan 2025	Reliance Industries and NVIDIA announce AI infrastructure partnership; USD 1.16B government AI investment commitment; GPU cluster deployment.	USD 1.16B+	Technology licensing; US export control compliance for H100/H200 chips; IP ownership allocation.

Date	Transaction	Value	Legal Structuring Note
Sep 2024	Princeton Digital Group deploys USD 1B across Chennai CH1 campus expansion and Mumbai MU1 capacity addition.	USD 1B	Land acquisition due diligence; construction contract negotiation; REIT monetisation structuring.
2025	Lumina CloudInfra (backed by Blackstone) and Panchshil Realty plan 500 MW AI-optimised campus in Navi Mumbai.	Undisclosed	SEBI REIT/InvIT eligibility assessment; real estate JV; pre-development planning approvals.

Source: JLL Capital Markets; Savills India; company announcements. KSK Analysis.

4.3 Legal Structures for Market Entry

Foreign investors and operators entering the Indian data center market have a range of structuring options, each presenting distinct legal, tax, regulatory, and operational trade-offs. The optimal structure is determined by the investor's strategic intent, the identity of its Indian counterparty (if any), the intended customer base, the regulatory classification of the workloads to be hosted, and long-term capital exit considerations. The principal available structures are analysed below.

Wholly Owned Subsidiary (WOS).
The most common entry structure for well-capitalised foreign operators is the incorporation of an Indian private limited company under the Companies Act, 2013, with 100% foreign equity held by the parent or a holding intermediate incorporated in a treaty-efficient jurisdiction (typically Singapore, Mauritius, or the Netherlands). Data center infrastructure falls under the automatic route for FDI under Schedule I of the Foreign Exchange Management (Non-Debt Instruments) Rules, 2019, with no sectoral cap and no prior government approval required, subject to compliance with FEMA pricing guidelines on share issuance and downstream investment regulations. The WOS structure provides maximum operational control, simplifies regulatory filings, and facilitates direct contracting with enterprise and hyperscaler clients. Tax considerations include the applicability of the Base Erosion and Profit Shifting (BEPS) framework to intra-group service charges, interest on shareholder loans (subject to thin capitalisation limits under Section 94B of the Income Tax Act), and the availability of tax treaty benefits on dividend repatriation.

Joint Venture with Indian Strategic Partner.
Joint ventures with established Indian conglomerates or real estate platforms as exemplified by the Google-Adani alliance, the Colt DCS-RMZ Corp joint venture, and the AdaniConneX structure are the preferred model where the foreign party seeks land access, domestic regulatory relationships, grid connectivity, or accelerated permitting that an Indian partner can provide. The legal documentation of a JV requires careful attention to: shareholder agreement governance (reserved matters, deadlock resolution, and anti-dilution protections); the FEMA pricing rules applicable to any secondary transfer of shares between the parties; Competition Commission of India (CCI) merger control notification requirements where the parties' combined thresholds exceed the prescribed financial limits; and the exit mechanics, including tag-along, drag-along, and put/call option enforceability under Indian law (note: options on equity shares of private companies became enforceable following the Supreme Court's decision in Vodafone International Holdings BV v. Union of India and subsequent SEBI and RBI guidance).

V. Contractual and Transactional Considerations

5.1 Data Center Lease and Colocation Agreements

The negotiation of data center colocation and lease agreements in India requires navigation of several overlapping legal regimes that do not arise in comparable Western jurisdictions. The Transfer of Property Act, 1882 governs the underlying lease, while the DPDP Act, the IT Act, sector-specific regulations, and the Electricity Act impose independent compliance obligations that must be addressed in contract.

Table 5: *Colocation Agreement — Material Negotiation Points*

Risk	Severity	Legal Implication	KSK Advisory
State incentive policy reversal	Medium	Loss of stamp duty exemption, power subsidies, or interest subvention post-commitment; adverse impact on projected IRR.	Seek legally binding State Investment Agreement with stabilisation provisions. Avoid reliance solely on policy circulars.
US export controls on advanced AI chips	Medium	Delay in GPU cluster delivery; project timeline and revenue commitment risk; potential contractual breach vis-à-vis tenants.	Advance procurement; alternative supplier qualification; robust FM provisions in hardware supply contracts.
GST on data center services and ITC chain optimisation	Low	18% GST on colocation services; input tax credit availability depends on legal structure and customer profile.	Optimise ITC chain at structuring stage. SEZ structures eliminate GST on export-linked revenue.

Source: KSK Legal Risk Assessment. Critical = immediate material risk of licence-level or INR 200 crore+ consequence; High = significant financial or operational risk; Medium = manageable with appropriate planning; Low = routine.

	only; no physical site inspection rights.	with 48 hours' notice. Access rights sufficient to satisfy regulatory examination by RBI, SEBI, or IRDAI.
Exit and Data Portability	Standard 12-month termination notice; no operator obligation to facilitate data migration.	Operator-assisted migration plan incorporated as contractual schedule. ISO 27001-certified data destruction certificate on termination. DPDP Act-compliant erasure confirmation.

5.2 Power Purchase Agreements - Renewable Energy

Power economics are the single most significant determinant of long-term data center operating economics in India. Power costs represent 60–70% of ongoing operational expenditure, and the differential between grid tariff (INR 6–9 per kWh for commercial consumers) and long-term renewable PPA tariff (INR 2.50–3.50 per kWh for round-the-clock solar-plus-storage structures) can reduce power cost by 30–40%, transforming the economics of competitive colocation pricing.

Long-term renewable PPAs in India are governed by the Electricity Act, 2003, state electricity regulatory commission regulations, and the Central Electricity Regulatory Commission framework. The legal negotiation of such agreements requires careful attention to: open access charges and wheeling fees, which vary by state and can add INR 0.50–2.50 per kWh to the effective cost; Renewable Energy Certificate compliance under the Renewable Purchase Obligation framework; group captive power structure requirements (minimum 26% equity participation and 51% energy offtake); banking provisions governing the treatment of generation in excess of concurrent consumption; and change- in-law protections. KSK advises that change-in-law clauses in renewable PPAs should be carefully calibrated - neither so broad as to create an exit right on any regulatory development, nor so narrow as to leave one party bearing the entire risk of adverse regulatory change.

5.3 Land Acquisition and Real Estate

Data center campuses of the scale demanded by hyperscale operators - typically 15–50 acres for a 100 MW+ facility - require significant land acquisition in the primary hub markets. Title due diligence in India requires examination of revenue records, mutation entries, encumbrance certificates, and property tax receipts across a minimum 30-year period. Agricultural land conversion to non-agricultural use - necessary in most development scenarios - requires a formal conversion order from the relevant state revenue authority, a process that typically requires 6–18 months and should be initiated before execution of a binding sale agreement.

Environmental clearances under the EIA Notification, 2006 are required for data center projects in most configurations, with Category B2 appraisal by the State Environment Impact Assessment Authority (SEIAA) being the typical pathway. KSK recommends concurrent commencement of environmental and land conversion processes at the earliest possible stage to avoid sequential delay. Fire safety NOCs and building plan approvals from the relevant municipal or development authority should be obtained before operational commencement; post-commissioning enforcement action on building consent issues has created material operational disruption for operators in prior cycles.

Development Agreement Structures

Where outright land acquisition is not feasible within a project timelinetypically due to pending agricultural conversion or ongoing title remediationa development agreement with the landowner, structured as a licence rather than a lease to avoid Transfer of Property Act registration requirements, can permit construction commencement while title work is completed. This structure requires careful legal documentation to ensure that the developer's investment is protected against landowner default and that the conversion order, once obtained, is capable of being acted upon by the developer without further landowner cooperation. KSK has successfully deployed this structure on multiple data center projects in Maharashtra and Tamil Nadu where aggressive commissioning timelines have required parallel-pathing of construction and title remediation.

VI. Risk Assessment

The following table summarises the principal legal, regulatory, and structural risks facing data center operators, investors, and occupiers in India as of March 2026, together with KSK's assessment of risk severity and recommended advisory action. Risk severity is assessed by reference to the probability of materialisation and the magnitude of potential legal, financial, or operational consequence.

Table 6: *Legal Risk Assessment — India Data Center Market (March 2026)*

Risk	Severity	Legal Implication	KSK Advisory
Failure to achieve DPDP compliance by 13 May 2027	Critical	Penalties to INR 250 crore per contravention; DPBI enforcement; reputational exposure; potential director liability.	Establish compliance programme office immediately. Commission gap assessment and legal mapping of data flows. Do not defer to the 2027 deadline.
CERT-In 6-hour incident reporting breach	Critical	Criminal liability under IT Act; regulatory enforcement by CERT-In; potential CII designation consequences.	Ensure 24x7 SOC with documented incident detection and response protocols. Contractual cooperation clause in all tenant agreements.
RBI payment data localisation — occupier non-compliance	Critical	RBI has authority to revoke payment system licence; personal liability for authorised signatories.	Verify all RBI-regulated occupiers process payment data exclusively on India-resident infrastructure. Document compliance confirmation in occupancy agreements.
Adverse government notification restricting cross-border data transfers	High	Retrospective restriction on currently permitted data flows; SDF-specific obligations without adequate preparation time.	Map all cross-border data flows now. Identify categories most likely to be notified. Build contingency capacity and contractual flexibility.
Power supply disruption and SLA breach claims	High	Force majeure disputes; customer compensation claims; contractual credit obligations; potential tenant termination rights.	Negotiate FM carve-outs to exclude foreseeable grid events. Procure group captive renewable with battery storage.
Environmental clearance delay or revocation	High	Project delays of 12–24 months; sunk construction cost; lender covenant breach; potential stop-work order.	Engage specialised EIA consultant at project inception. Apply for EC concurrently with land acquisition.
Competition Act merger control — consolidation transactions	Medium	CCI approval required for transactions above prescribed thresholds; gun-jumping risk for premature implementation.	File notification with CCI at MoU stage. Build 90–150 day regulatory clearance period into transaction timeline.

Risk	Severity	Legal Implication	KSK Advisory
State incentive policy reversal	Medium	Loss of stamp duty exemption, power subsidies, or interest subvention post-commitment; adverse impact on projected IRR.	Seek legally binding State Investment Agreement with stabilisation provisions. Avoid reliance solely on policy circulars.
US export controls on advanced AI chips	Medium	Delay in GPU cluster delivery; project timeline and revenue commitment risk; potential contractual breach vis-à-vis tenants.	Advance procurement; alternative supplier qualification; robust FM provisions in hardware supply contracts.
GST on data center services and ITC chain optimisation	Low	18% GST on colocation services; input tax credit availability depends on legal structure and customer profile.	Optimise ITC chain at structuring stage. SEZ structures eliminate GST on export-linked revenue.

Source: KSK Legal Risk Assessment. Critical = immediate material risk of licence-level or INR 200 crore+ consequence; High = significant financial or operational risk; Medium = manageable with appropriate planning; Low = routine.

The risk profile of the Indian data center market has evolved materially between 2023 and 2026. Regulatory risk has become more quantifiable following the notification of the DPDP Rules, which provides a defined compliance timeline and a known penalty framework. Power risk has decreased as the renewable energy procurement market has matured and long-term PPA structures have become standardised. Geopolitical risk particularly US export controls on advanced AI chips has increased and requires active management through advance procurement planning and diversified hardware supply chains.

Risk Mitigation Framework

KSK recommends that data center operators and investors adopt a structured risk register approach, with each identified risk assigned an owner, a monitoring mechanism, and a defined mitigation action. Critical risks should be subject to quarterly board-level review. The DPDP compliance programme should be treated as a standalone workstream with executive sponsorship and independent progress reporting. The 14-month runway remaining as of March 2026 is the minimum necessary for a complex processing organisation to achieve full compliance by May 2027.

From an investment due diligence perspective, KSK advises acquirers of Indian data center businesses to use the above risk assessment as a structured checklist. Critical and High-risk items should be backed by specific warranties, representations, or indemnities, along with escrow or price adjustment protections where risks are not fully quantifiable at signing. Particular caution is warranted around DPDP compliance, which remains the most significant and often under-disclosed risk, making independent verification essential.

VII. Emerging Trends

7.1 Artificial Intelligence Infrastructure

The proliferation of AI-optimised data center infrastructure - characterised by GPU cluster deployments, high-performance interconnect fabric, and liquid or direct-to-chip cooling systems - creates a novel set of legal questions for which India's regulatory framework has, as yet, provided limited guidance. MeitY published a Discussion Paper on India's AI Governance Framework in 2024, with a formal regulatory instrument anticipated in the second half of 2026. In the interim, AI workloads are subject to the general provisions of the DPDP Act and the IT Act, without any AI- specific safe harbours or carve-outs.

For data center operators, the most immediate legal implication of AI workload hosting relates to liability allocation for outputs generated by AI systems processed on their infrastructure. In the absence of specific legislation, general principles of contract and tort law apply. KSK advises that colocation and cloud service agreements should contain an explicit AI workload liability addendum that: defines AI workloads as a distinct service category; allocates responsibility for algorithmic outputs as between operator and occupier; addresses the DPDP Act Rule 13 requirement for annual algorithmic risk assessments for Significant Data Fiduciaries that use AI systems; and establishes compliance representations with respect to US export control requirements applicable to advanced semiconductor hardware.

7.2 Sustainability and ESG Obligations

Sustainability obligations for India-based data center operators have transitioned in the course of three years from voluntary aspiration to commercial and regulatory imperative. The SEBI Business Responsibility and Sustainability Reporting (BRSR) Core framework, mandatory for the top 1,000 listed companies from FY 2023–24, requires verified disclosure of energy consumption, water usage, and Scope 1 and 2 greenhouse gas emissions. The Bureau of Energy Efficiency (BEE) is developing a data center-specific energy performance standard that, when enacted, will establish mandatory Power Usage Effectiveness benchmarks - anticipated at sub-1.5 PUE for new facilities - with consequences for continued operating permits.

From a commercial standpoint, hyperscaler tenants increasingly impose sustainability requirements as conditions of pre-lease execution: verified commitments to 100% renewable energy coverage, net- zero carbon roadmaps with third-party assurance, water-efficient cooling designs, and compliance with GRIHA or IGBC green building standards. Operators without such credentials are effectively excluded from hyperscaler RFP processes at a growing proportion of campuses. Legally, this trend creates consequential representation and warranty risk in sale transactions and InvIT listings where

environmental credentials are included in marketing materials without adequate underlying verification.

The E-Waste (Management) Rules, 2022 impose Extended Producer Responsibility (EPR) obligations on hardware producers, importers, and brand owners. Data center operators who take title to IT hardware must hold EPR certificates and ensure compliant IT asset disposition (ITAD) arrangements. Hardware lifecycle contracts should contain explicit EPR compliance warranties and indemnities, and ITAD service providers should be contractually required to maintain and provide EPR documentation at each disposal event.

Water Usage and Cooling Efficiency

Water consumption has emerged as the second most significant ESG metric for Indian data center operators, following energy. Evaporative cooling systems which remain prevalent in Indian data centers due to their cost-effectiveness relative to mechanical cooling consume approximately 1.8-3.5 litres of water per kWh of IT load, placing large campuses among the most significant commercial water users in their local jurisdictions. The Water (Prevention and Control of Pollution) Act, 1974 and state-level groundwater regulations impose extraction limits and discharge standards that operators must comply with, and hyperscaler tenants are increasingly requiring Water Usage Effectiveness (WUE) disclosures and targets as a condition of pre-lease execution. KSK advises operators to complete a water risk assessment including mapping of local regulatory extraction limits and projected water stress under climate change scenarios at the site selection stage, before land acquisition commitments are made.

Green Financing and Sustainability-Linked Instruments

The growth of green bond and sustainability-linked loan (SLL) markets in India has created a meaningful financing incentive for data center operators who can demonstrate verifiable ESG credentials. The Securities and Exchange Board of India's Green Bond Framework and the Reserve Bank of India's guidelines on Green Deposits provide the regulatory foundation for green capital raising, and several Indian data center operators have successfully accessed international green bond markets at a cost of capital 30-60 basis points below equivalent conventional debt. To qualify, operators must demonstrate use of proceeds alignment with the Green Bond Principles and provide independent second-party opinions on their sustainability frameworks. KSK has advised on green financing structures for data center assets and recommends that operators engage sustainability advisers to develop credible frameworks before approaching capital markets, as greenwashing risk including SEBI enforcement action for misleading ESG disclosures live and increasing concern.

VIII. KSK Strategic Recommendations

For Institutional Investors

Investors evaluating data center exposure in India should treat DPDP compliance status as a primary due diligence workstream, equivalent in importance to financial and technical due diligence. Compliance gaps in an acquisition target represent not merely legal risk but a material valuation discount: remediation costs, regulatory uncertainty, and the management distraction of a compliance build-up in an operational business are all quantifiable impairments to enterprise value. KSK recommends that LOI or term sheet documentation for any Indian data center acquisition include a representation as to DPDP compliance programme status, and that a full legal audit of data flows, vendor DPAs, and breach notification readiness be completed before conditions are satisfied.

On power risk: investments should be stress-tested against a scenario in which grid tariff increases by 20% and open access charges increase by INR 0.75 per kWh - both of which are credible regulatory outcomes in the current period. Long-term renewable PPAs with group captive structures and battery storage backup, negotiated before financial close, provide the most defensible cost model and should be treated as a condition precedent to investment, not a post-acquisition optimisation.

State incentive packages should be treated with caution in financial models. Policy circulars are, in Indian administrative law, revocable instruments and do not carry the legal certainty of a bilateral investment agreement. Investors should seek legally binding State Investment Agreements with explicit stabilisation provisions before relying on state incentives in underwriting assumptions.

For Data Center Operators

The 13 May 2027 DPDP compliance deadline demands immediate, structured action. KSK's assessment of the programme of work required - gap analysis, data flow mapping, consent notice redesign, vendor contract remediation, DPO appointment, security infrastructure uplift, breach notification protocol design, and staff training - is that 18–24 months of sustained programme office effort is the realistic minimum for a complex operator processing personal data at scale. Operators who have not yet commenced this programme are, as of March 2026, already behind schedule.

On AI workload contracts: the combination of heightened liability exposure, export control compliance requirements, novel cooling infrastructure obligations, and anticipated regulatory change means that standard master service agreements drafted for conventional IT workloads are not adequate for AI deployments. An AI workload addendum - addressing GPU-specific SLAs, liquid cooling obligations, liability allocation for model outputs, hardware export control representations, and algorithmic audit cooperation obligations - should be developed as a standard commercial document and appended to new and renewing agreements with AI-deploying occupiers.

For Enterprise Occupiers and Cloud Users

Regulated entity occupiers -particularly those in the BFSI sector - should immediately commission a data residency and flow mapping exercise to confirm compliance with the independently operative sectoral mandates of the RBI, SEBI, and IRDAI. The consequences of non-compliance (licence revocation in the most severe cases) are disproportionate to the cost of compliance, and KSK is not aware of any regulator in the current environment that treats good faith as a complete defence to a localisation breach.

On vendor agreements: occupiers should ensure that all cloud service and colocation agreements include DPDP Act-compliant Data Processing Agreements that expressly designate the operator as a Data Processor, define processing instructions, specify security standards, impose a 24-hour notification obligation to the occupier on breach detection, and include an operator obligation to cooperate in regulatory examinations. These provisions are not currently market standard in India and must be negotiated affirmatively.

KSK's overarching strategic assessment for the period through 2028 is that the Indian data center market rewards speed and preparation in equal measure. The operators and investors who will capture the most value are those who have completed their DPDP compliance programmes ahead of the 2027 deadline, secured long-term renewable power purchase agreements at current market rates, and established reliable relationships with state government infrastructure teams in the two or three hub markets where they intend to operate at scale.

KSK's Service Offering

King Stubb & Kasiva's Technology, Media & Telecommunications practice provides end-to-end legal support across the data center investment lifecycle: regulatory compliance advisory (DPDP, CERT-In, sectoral localisation); transaction structuring and execution (FDI, JV, InvIT, M&A); land acquisition due diligence and real estate documentation; power purchase agreement negotiation; colocation agreement drafting and negotiation; and ongoing regulatory liaison. Our team has advised on transactions representing in excess of USD 3 billion in data center investment value across Mumbai, Chennai, Bengaluru, Hyderabad, and the Delhi-NCR corridor.

For further information on any aspect of this report, or to discuss how KSK can support your India data center strategy, please contact info@ksandk.com or visit the website at www.ksandk.com

IX. Appendix: Principal Legislation Governing Data Centers in India

Table 7: *Principal Legislation — India Data Center Sector*

Legislation	Year	Authority	Primary Relevance to Data Centers
Digital Personal Data Protection Act	2023	MeitY / DPBI	Comprehensive data protection framework; consent obligations; breach notification; cross-border transfers; Significant Data Fiduciary regime.
Digital Personal Data Protection Rules	2025	MeitY / DPBI	Operationalises DPDP Act; 18-month compliance runway to May 2027; constitutes DPBI; establishes algorithmic audit requirements for SDFs.
Information Technology Act (as amended)	2000 / 2008	MeitY / CERT-In	Section 43A sensitive data obligations; CERT-In incident reporting; Section 70 Critical Information Infrastructure designation powers.
IT (Reasonable Security Practices) Rules	2011	MeitY	Defines sensitive personal data; prescribes security practices for bodies corporate processing such data.
Electricity Act	2003	CERC / SERCs	Open access and power procurement framework; renewable purchase obligations; third-party sale and group captive power structures.
Environment Protection Act + EIA Notification	1986 / 2006	MoEFCC / SEIAA	Environmental clearance process for large data center projects; hazardous waste management obligations.
Companies Act	2013	MCA / NCLT	Incorporation and governance of Indian data center entities; foreign company registration; beneficial ownership disclosure.
Foreign Exchange Management Act	1999	RBI / Enforcement Directorate	FDI entry and sectoral caps; repatriation of profits; External Commercial Borrowing conditions; FEMA pricing guidelines on share transfers.
Competition Act	2002	Competition Commission of India	Merger control for acquisitions above prescribed financial thresholds; anti-competitive conduct in colocation markets.
SEBI InvIT Regulations	2014	SEBI	Registration, listing, and ongoing compliance for Infrastructure Investment Trusts holding data center assets.
SEZ Act and Rules	2005 / 2006	Ministry of Commerce / BOA	Customs duty and GST exemptions for IT/ITES data centers operating in or serving Special Economic Zones.
E-Waste (Management) Rules	2022	CPCB / SPCBs	Extended Producer Responsibility obligations; IT hardware disposal and ITAD compliance requirements.
RBI Master Direction on Storage of Payment System Data	2018	Reserve Bank of India	Mandatory in-country storage of all payment system data; currently operative with no grace period.

Source: KSK Legal Research, March 2026. This list is indicative and not exhaustive.

Contacts

Jidesh Kumar
(Managing Partner)
jidesh@ksandk.com

Rajesh Sivaswamy
(Senior Partner)
rajesh@ksandk.com

Adnan Siddiqui
(Partner)
adnan@ksandk.com

Asha Kiran Sharma
(Partner)
asha@ksandk.com

Vivek Boray
(Partner)
vivek@ksandk.com

Abhishek Paliwal
(Partner)
abhishek.paliwal@ksandk.com

Aurelia Menezes
(Partner)
aurelia@ksandk.com

Nivedita Bhardwaj
(Partner)
nivedita@ksandk.com

Sindhuja
(Partner)
sindhuja@ksandk.com

Prithiviraj Nathan
(Partner)
prithivi@ksandk.com

Our Offices

New Delhi

RNM Tower, 5th Floor, Metro pillar no 331, i4, B 1, NH-19, Mohan Cooperative Industrial Estate, New Delhi, 110044
Tel: +911141318190/41032969
Email: delhi@ksandk.com

Bangalore

1A, 1B, 2B & 3B Lavelle Mansion, 1/2, Lavelle Road, Bangalore
Tel: +91 80 41179111/41179222,
Email: bangalore@ksandk.com

Chennai

211, Alpha Wing, Second Floor, Raheja Towers, #177, An / na Salai, Chennai
Tel: +91 44 28605955/28606955
Email: chennai@ksandk.com

Mumbai(1)

61, Atlanta Building, Jamnalal Bajaj Road, Nariman Point, Mumbai
Tel: +91 22 62372076/22020080
Email: mumbai@ksandk.com

Mumbai(2)

301A, 3rd Floor, Piramal Tower, Peninsula Corporate Park, Lower Parel, Mumbai -400013
Tel: +91 22 35253198
Email: mumbai@ksandk.com

Pune

Bootstart Cowork, 1st Floor, Arcadian Building Plot No 12, Lane 5A, Koregaon Park, Pune
Tel: +91 9833555232
Email: pune@ksandk.com

Mumbai(3)

802, 8th Floor, REMI COMMERCIO, Shah Industrial Estate, Veera Desai Road, Andheri Link Road, Behind Yash Raj Studio, Andheri (West), Mumbai - 400 053
Tel: +91 2235253198
Email: mumbai@ksandk.com

Kochi

1st Floor, Manavalan Building, Banerji Road, Ernakulam, Kochi
Tel: +91 484-3592950
Email: kochi@ksandk.com

Hyderabad

609, Shangrila Plaza, Road no. 2, Banjara Hills, Hyderabad, Telangana
Tel: +91 40 48516011/+91 40 48506011
Email: hyderabad@ksandk.com

KING STUBB & KASIVA
ADVOCATES AND ATTORNEYS