HyperNext Data Centers

RESEARCH PAPER

HN-RP-003

India's Sovereign AI Cloud

A framework for data residency that survives audit

Three layers of sovereignty. MeitY and RBI in practice. What the questions actually are.

This is what is Next.

Series	HyperNext Research
Paper	HN-RP-003
Issued	12 December 2025
Version	1.0
Classification	Public release
Citation	HyperNext Research, HN-RP-003

India's Sovereign AI Cloud

This paper is part of the HyperNext Research series. Methodology, assumptions, and source data are stated openly so other operators can reproduce the analysis on their own facilities. Citation as "HyperNext Research, HN-RP-003" is welcome.

Contents

1. The phrase has become unclear

ABSTRACT

"Data residency" and "sovereign cloud" have become loose terms in Indian cloud procurement conversations. The looseness now matters. The Digital Personal Data Protection Act of 2023, the RBI data localisation directives for payment systems, the MeitY guidelines for non-personal data, and the IT Act recent amendments together create a regulatory environment in which the specific layer at which sovereignty applies determines whether a given deployment is compliant or not. This paper proposes a three-layer framework to make the conversation more precise. Where the data physically sits is one question. Which jurisdiction's law governs access to it is a second. Who has operational control over the systems holding it is a third. These three questions can be answered independently, and the wrong answer at any layer creates regulatory exposure regardless of the other two. We describe the HyperNext Hyper 7 sovereign cloud platform as a concrete example of one set of design decisions across the three layers. The framework is non-proprietary.

A cloud workload running on Indian soil, in an Indian data centre, owned by an Indian operator, can still fail Indian regulatory tests if the operational control is exercised from abroad. The opposite combinations exist too. This paper is about why that matters and what to do about it.

The regulatory landscape since 2018

Indian data sovereignty regulation has tightened in three waves. The 2018 RBI directive on payment system data localisation required the full lifecycle of payment data for transactions in India to be stored only in India, with limited and time-bound exceptions for cross-border processing. The 2022 amendments to the IT Rules expanded scope to social media intermediaries and added breach reporting requirements. The 2023 Digital Personal Data Protection Act introduced a framework for personal data that applies to all controllers handling Indian residents' data, including a notion of "trusted geography" cross-border transfers and a categorisation of data fiduciaries by sensitivity.

The MeitY guidelines for non-personal data, in their current form as of 2024, address a category the DPDP Act does not. Business data, sectoral data, and machine-generated data that may not be personally identifiable but is still considered to have national strategic value. Sovereign cloud, as commonly used in 2026, refers to the combination of all of these requirements. A cloud platform that satisfies residency, access control, and operational control requirements across personal, non-personal, and payment data at the same time.

2. The three layers

Layer one: physical residency

The first question is straightforward and is the one most cloud providers answer well. Where, geographically, does the data physically sit. On which servers, in which data centres, in which countries. US hyperscalers compete at this layer in their Indian regions. AWS Mumbai and Hyderabad, Azure Pune and Hyderabad, GCP Mumbai and Delhi. All are layer-one compliant for residency. Data put into an India region of any of these providers physically stays in India under normal operating conditions.

The complications at layer one are around replication, disaster recovery, backup, and edge processing. A workload in an India region that replicates its database synchronously to a Singapore region for DR has technically left Indian residency. A workload whose backups are cross-region replicated to a US Glacier tier for cost optimisation has technically left Indian residency. Edge processing that pre-summarises data before it reaches the India region creates a residency question about the pre-summarised data. Layer-one compliance needs not just the primary residency choice but a careful audit of all secondary data movement paths.

Layer two: jurisdictional control

The second question is harder. Even when data physically sits in India, what jurisdiction's law governs access to it? Specifically, can a foreign government compel the cloud provider to produce the data, regardless of where it sits? The US CLOUD Act of 2018 explicitly extends the jurisdiction of US courts over data held by US-headquartered cloud providers worldwide, including data held in foreign cloud regions. Data in an Indian region of a US-headquartered hyperscaler can be subject to subpoena under US law, even though it is physically in India. The provider is legally obligated to respond, regardless of Indian law's position.

The Indian regulatory response has been to require, for certain categories of sensitive data, that the controlling entity be subject to Indian jurisdiction first. The RBI payment data directive, in practice, requires the cloud provider holding the data to be either headquartered in India or operate through an Indian subsidiary structured such that Indian law has primary jurisdictional claim. The DPDP Act is more nuanced. It permits cross-border transfers to "trusted geographies" but reserves the right to designate categories of data for which only Indian-jurisdiction controllers are permitted. That list has been growing.

Layer-two compliance is therefore not just about where the data sits, but about who could be compelled to produce it and by whom. A workload that needs strong layer-two sovereignty must run on a provider whose corporate structure makes it primarily accountable to Indian law. US-headquartered hyperscalers cannot fully compete at this layer. Indian sovereign cloud platforms have a structural advantage here.

Layer three: operational control

The third question is the one most often missed. Who exercises operational control over the systems holding the data? Where are the engineers who can administer the platform located? From what jurisdiction are the firmware updates pushed? In an incident, who has the technical ability to access the system in ways the contractual layers do not permit?

This matters because operational control is the layer at which contractual sovereignty can be bypassed. A platform contractually subject to Indian law with data physically in India can still be operationally compromised if the platform administrators sit abroad and are subject to a foreign government compulsion. A platform whose firmware updates come from a foreign engineering centre has an ongoing supply chain access route that contractual terms cannot foreclose. A platform whose break-glass administrative access needs support from a foreign team has an availability dependency on that team jurisdiction.

Indian regulation has begun to address this. The MeitY 2024 guidance on critical information infrastructure protection requires operational control of designated CII systems to be exercised entirely from within India, by personnel under Indian law jurisdiction, with all administrative access logged and auditable within Indian jurisdiction. The categories of CII have expanded year over year. The practical effect: a growing list of workloads now needs layer-three sovereignty as well as layers one and two.

3. The questions to ask

Operators procuring cloud services for regulated workloads should ask the following questions of any prospective provider. Listed in the order practical risk usually increases.

#	Question	Layer
1	In which countries are the primary servers physically located?	1
2	What is the complete list of secondary data locations including DR, backup, replication, and edge?	1
3	Under which country's corporate law is the provider primarily incorporated?	2
4	Is the Indian operating entity a subsidiary with independent legal capacity, or a branch of a foreign parent?	2
5	What is the provider policy and history on responding to foreign-government compulsory production requests for Indian data?	2
6	From which physical location is administrative access to the systems exercised in normal operations?	3
7	From which physical location is break-glass access exercised in incidents?	3
8	Are firmware and operating system updates to the underlying hardware controlled from within India?	3
9	Are encryption keys generated, stored, and rotated within Indian jurisdiction?	2 and 3
10	What is the full chain of personnel who have, in technical fact, the ability to access the platform data plane?	3

A provider that gives unambiguous answers to all ten questions is in a position to make sovereignty claims. A provider that requires conditional answers or defers to corporate-level policy on any of them is at risk on the corresponding layer. The questions are not hostile. They are the questions a CISO at a regulated bank or a CIO at a government agency should be asking as a matter of due diligence.

THE THREE-LAYER TEST

- Layer 1, residency: where does the data sit, including all secondary copies?
- Layer 2, jurisdiction: which country's law governs compelled access to the data?
- Layer 3, operational control: who can technically reach the data, and from where?
- A workload is sovereign only if all three layers are satisfied. Failing any one layer is failing sovereignty.

4. The Hyper 7 architecture

Design decisions across the three layers

The HyperNext sovereign cloud platform, Hyper 7, is designed to give unambiguous answers to all ten questions in Section 3. The design decisions across the three layers are below.

Layer 1. All Hyper 7 primary servers sit in HyperNext Indian data centres. Phase 1 launch is at the Hyderabad campus. Primary capacity will move to Kakinada as Phase 2 comes online. DR runs to the Nava Raipur facility, which is specifically engineered as a DR site for AI workloads (the subject of a future paper in this series). Backups are tiered locally within the operating region. There is no cross-border replication of any tier of customer data under any normal operational mode.

Layer 2. Hyper 7 is operated by HyperNext Data Center Limited, an Indian Public Limited Company (CIN U63111TS2025PLC204792) with no foreign parent. The corporate structure is intentionally not a subsidiary of a foreign entity. There is no foreign-jurisdiction path through which compelled production of Hyper 7 customer data can be lawfully obtained. The platform is contractually and structurally subject to Indian law for all data access purposes.

Layer 3. Operational control of Hyper 7 is exercised from HyperNext network operations centres at the Hyderabad and (from 2028) Kakinada campuses. Administrative personnel are HyperNext employees subject to Indian law jurisdiction. Break-glass access procedures require dual control by two named personnel, both physically present at an Indian NOC at the time of access. Firmware and operating system updates to the underlying hardware are managed from within India. Vendor support engagements that need non-Indian personnel access run over recorded sessions with HyperNext personnel co-present and with audit trail. Customer-managed encryption keys live in Indian HSM clusters not accessible to HyperNext personnel without dual-control approval.

What customers do

The customer responsibility on a sovereign cloud platform is not zero. The platform can be configured in ways that defeat the sovereignty model. A customer-side replication tool copying data to a non-sovereign environment will do it. Integrating the platform with a SaaS application whose own jurisdiction is non-sovereign will do it. Compliance is shared between platform and customer.

Hyper 7 provides a sovereignty conformance certification on a per-workload basis. The platform validates the customer deployment configuration against the three-layer test and issues a continuously updated conformance attestation that can be presented to auditors. This is not a one-time check. It is a continuous attestation that re-validates whenever the configuration changes. Customers can rely on the attestation for their regulatory filings without having to re-derive the sovereignty argument from first principles.

5. What this looks like in practice

Three worked examples

Example A. A scheduled commercial bank KYC platform. The data is personal under DPDP, financial under RBI rules, and the bank is large enough to be a Significant Data Fiduciary. All three layers must be satisfied. Hyper 7 hosts the platform in Hyderabad primary with Nava Raipur DR. HyperNext is the data processor under Indian jurisdiction. Operational control is fully Indian. Customer-managed keys remain in the bank own HSM cluster. The conformance attestation covers the platform. The bank own compliance team covers the application-level configuration.

Example B. A non-bank financial company credit scoring AI. The data is personal under DPDP. The use case is not directly RBI-regulated, but the credit decisions affect financial inclusion and so the company chooses to operate under sovereign cloud as a defensive position even where strictly not required. Hyper 7 hosts the inference platform in Kakinada with the Vera Rubin Ultra NVL576 capacity that the workload needs. The model itself remains the customer property under their own license and is encrypted at rest with customer-managed keys.

Example C. A government department internal analytics workload. The data is non-personal but designated as CII under MeitY guidance. Sovereignty requirements include layer three explicitly. Hyper 7 hosts the workload in a dedicated tenancy in Hyderabad with a restricted operational team subject to additional security clearance. The break-glass procedure for this tenant requires three-person concurrence rather than two.

Where the framework will need to evolve

The three-layer framework holds up against current Indian regulation. It will not stay sufficient indefinitely. Two pressures will reshape it. The supply chain layer is becoming a separate sovereignty concern. Not just the data but the hardware on which the data is processed has provenance questions that current law does not fully address. The AI-model layer is emerging as a fourth question. Where the model was trained, what data trained it, and which jurisdiction has claims on the resulting weights will become a sovereignty layer of its own. Both will be subjects of subsequent research papers in this series. For now, the three-layer test is sufficient for almost all 2026 procurement decisions.

HEADLINES

- Sovereign cloud needs correct answers at three independent layers: residency, jurisdiction, and operational control.
- Each layer can fail without the others failing. All three must hold for the workload to be sovereign.
- The ten questions in Section 3 are the practical test. Any provider claiming sovereignty for Indian regulated workloads should be able to answer all ten without conditional language.
- The HyperNext Hyper 7 platform is designed to give unambiguous answers at all three layers, including continuous conformance attestation at the per-workload level.
- The framework will need to extend to supply chain and AI-model layers as the regulatory environment evolves.

6. Detailed regulatory mapping

The three-layer framework in Section 2 is the structural argument. The mapping below is the practical one. Each major Indian regulation maps to specific layer requirements. Operators evaluating sovereign cloud should be able to walk through this mapping for any workload.

Digital Personal Data Protection Act, 2023

Section	Provision	Layer mapping
5	Notice requirements for personal data processing	Procedural, no infra implication
6	Consent for processing	Procedural
8	General obligations of Data Fiduciary	Layer 2 (jurisdictional control of fiduciary)
10	Additional obligations of Significant Data Fiduciary	Layers 2 and 3 (audit, breach reporting, DPO presence)
16	Cross-border transfer restrictions	Layer 1 (residency for non-trusted geographies)
17	Government access to personal data	Layer 2 (jurisdictional jurisdiction must be Indian)
33	Children's data and verifiable consent	Procedural

The most important DPDP provisions for sovereign cloud architecture are Sections 16 and 17. Section 16 reserves the right for the central government to notify categories of personal data that cannot be transferred to designated countries. The list has been progressively expanded since the Act took effect. Section 17 establishes the framework under which Indian authorities can lawfully access personal data held by data fiduciaries. Together they make clear that the controlling entity over the data must be subject to Indian jurisdiction first.

RBI Storage of Payment System Data directive, 2018 (with subsequent clarifications)

The 2018 RBI directive remains the most demanding Indian regulation for sovereign cloud purposes. The directive requires that "the entire data relating to payment systems operated by them" be stored only in a system located in India. The 2018 FAQ clarified that this applies to the full lifecycle of payment data: storage, processing, transmission, and backup.

Limited exceptions exist for cross-border processing for a specific transaction (where the foreign leg of the transaction is being settled abroad) but the operational data must return to India within 24 hours and the

foreign copy must be deleted.

The directive has been enforced through audit. Several RBI-regulated entities have been issued cure notices for non-compliant cloud arrangements between 2020 and 2024. The compliance posture is therefore not theoretical. It is enforced.

MeitY Critical Information Infrastructure protection guidelines, 2024

The MeitY CII guidelines establish a category of data and systems whose security has implications for national security or public order. CII designations are made on a case-by-case basis by the National Critical Information Infrastructure Protection Centre (NCIIPC). Once designated, the system must satisfy layer-three sovereignty: operational control entirely from within India, by personnel subject to Indian law, with administrative access logged within Indian jurisdiction.

The list of designated CII systems has expanded year over year. As of 2026, the categories include payment systems (full coverage), large healthcare records platforms, electoral systems, transport ticketing systems above a scale threshold, and selected enterprise platforms operating in sensitive sectors.

IT Act amendments, 2022 to 2024

The IT Act amendments expanded the scope of "intermediary" obligations and added breach reporting requirements. The most consequential changes for sovereign cloud are the 6-hour breach notification rule (CERT-In Directive of April 2022, with subsequent extensions) and the requirement for the appointment of an India-resident Chief Compliance Officer for designated significant intermediaries.

7. International comparison

India sovereignty requirements are not unique. Comparable regimes exist in the European Union, China, Russia, and a growing list of other jurisdictions. The comparison below helps situate the Indian framework and identifies where international hyperscalers face similar constraints elsewhere.

European Union

The EU framework operates through the General Data Protection Regulation (GDPR) for personal data and the Data Act (effective 2024) for non-personal data. GDPR Article 48 prohibits compliance with foreign government compulsion of EU personal data unless an international agreement specifically permits it. This creates a structural conflict with the US CLOUD Act that the courts have not fully resolved.

The EU sovereign cloud market has responded with "Gaia-X compliant" platforms that satisfy three layers comparable to the framework in this paper. Several European hyperscalers (OVH, Scaleway) compete primarily on this jurisdictional positioning. US hyperscalers have responded with EU sovereign cloud offerings under partnership with European entities (Bleu, Delos), where the operating entity is EU-incorporated and operationally separated from the US parent.

China

China data sovereignty framework runs under the Cybersecurity Law (2017), Data Security Law (2021), and Personal Information Protection Law (2021). The combined effect is strict layer-one residency for most categories of data, layer-two jurisdiction under Chinese law for any platform serving Chinese users, and layer-three operational control inside China for designated critical information infrastructure.

The compliance position for US hyperscalers in China is more constrained than in the EU. AWS China, Azure China, and Alibaba Cloud all operate through Chinese-incorporated entities under Chinese law, with infrastructure inside China, and with operational control exercised from China. The US parent has no operational access to the Chinese region.

The Indian regime is moving in a direction that resembles the Chinese framework more than the European one in terms of layer-three operational control requirements. The 2024 MeitY guidance on CII operational control is structurally similar to the Chinese CII framework, although the implementing detail is less prescriptive.

Russia

Russia personal data localisation law (Federal Law No. 242-FZ of 2014) is the original modern data residency regime. It requires personal data of Russian citizens to be stored in databases physically

located in Russia. The 2019 amendments expanded enforcement and added the operational control requirement that has subsequently been adopted in other jurisdictions.

Other jurisdictions

Brazil (LGPD 2018), South Korea (PIPA 2011), Vietnam (Cybersecurity Law 2018), and Indonesia (PDP Act 2022) all have residency or jurisdiction provisions of varying strictness. The trend is unambiguous: data sovereignty has moved from being a competitive position to being a compliance requirement in most major economies.

8. Hyper 7 architecture detail

Section 4 introduced the Hyper 7 platform. This section is the engineering-level detail an architect or auditor would want to see when evaluating whether the platform actually satisfies the three-layer test.

Physical architecture

Hyper 7 runs on dedicated HyperNext hardware in dedicated halls of the HyperNext data centres. The platform is not multi-tenant with non-Hyper-7 workloads at the hardware level. This is a deliberate isolation choice: it eliminates side-channel attack surfaces between Hyper 7 tenants and other HyperNext customers, and it simplifies the audit trail.

Phase 1 deployment is at the Hyderabad campus, on a dedicated 4-hall footprint within Building 2, with 1,200 racks at full build-out. Phase 2 (from Q1 2027) extends to dedicated capacity at the Kakinada AI Factory. The DR site at Nava Raipur is engineered to the same isolation standard.

Network architecture

The Hyper 7 network is segregated at the physical layer from non-Hyper-7 traffic. Each tenant tenancy is on a dedicated VLAN with hardware-enforced isolation. East-west traffic between tenants is blocked at the fabric level, not by software policy. Tenant ingress is through a dedicated edge zone with Indian-jurisdiction TLS termination.

The platform supports BYO IP address space and BYO BGP peering for tenants that need to integrate Hyper 7 capacity into their existing network architecture. Cross-connect into the carrier-neutral Meet-Me Room is available for tenants who need direct interconnection to specific carriers.

Key management architecture

The Hyper 7 key management service (KMS) provides three tiers of key custody. Platform-managed keys are generated and managed by HyperNext within HSMs at the Indian data centres. Customer-managed keys are generated by the customer and stored in dedicated HSM partitions allocated to that customer. Bring-your-own-key uses customer-controlled HSMs (typically on-premises in the customer environment) with the Hyper 7 platform accessing keys for cryptographic operations but never holding them in cleartext.

For workloads requiring the strongest sovereignty posture, the BYOK option ensures that even HyperNext personnel cannot decrypt the customer data. The price is operational dependency on the customer HSM availability.

Identity and access architecture

Hyper 7 administrative access is gated through a dedicated Privileged Access Management (PAM) layer. All HyperNext personnel administering Hyper 7 are HyperNext employees with India-based contracts and Indian-resident status. Access requires multi-factor authentication, session recording, and just-in-time elevation. The full session log is immutable and retained for the contractual audit period (typically 7 years).

Break-glass procedures (emergency access bypassing normal approval flow) require dual-control by two named personnel, both physically present at the Hyderabad or Kakinada NOC at the time of access, with the reason recorded in free text and reviewed at the next operational review.

Foreign vendor support engagements (where vendor personnel need temporary access for support purposes) operate under recorded session protocol. The vendor session is screen-recorded, the HyperNext supervisor is co-present in the session, the actions are logged at the OS level, and the access is revoked within the agreed support window.

Audit trail

Every administrative action on the Hyper 7 platform is recorded in an immutable audit log. The log structure is shown below.

```
AUDIT RECORD STRUCTURE
{
  "ts": "2026-06-03T11:23:45.123+05:30",
  "session": "ses_3kt9j2lkhsfd",
  "actor": {
    "id": "u_8273kh",
    "role": "platform-admin",
    "auth_method": "fido2+pam",
    "originating_ip": "10.84.12.7",
    "originating_location": "HYD-NOC-01"
  },
  "subject": {
    "tenant": "t_9f1bxq",
    "resource_class": "hsm-partition",
    "resource_id": "hsm-p-118"
  },
  "action": "rotate-master-key",
  "result": "success",
  "approval": {
    "required": true,
    "approver_id": "u_2810sd",
    "approver_role": "shift-lead",
    "approval_ts": "2026-06-03T11:23:42.115+05:30",
    "reason": "scheduled-annual-rotation"
  },
  "hash_prev": "0x8a3b...",
  "hash_self": "0x4c1f..."
}
```

The hash_prev and hash_self fields form a hash chain across records. Any tampering with a record breaks the chain at that record and all subsequent records. The chain is verified continuously and the head hash is exported daily to a cold-storage write-once medium for forensic purposes.

9. References and standards

Indian regulatory texts and the international standards referenced in this paper are listed below. Where the official text is available online, the URL is provided in the published HTML version of this paper.

Indian regulations

- The Digital Personal Data Protection Act, 2023. Ministry of Electronics and Information Technology.
- RBI Notification DPSS.CO.OD No. 2785/06.08.005/2017-2018, "Storage of Payment System Data", April 2018, with subsequent FAQ clarifications.
- The Information Technology Act, 2000, as amended through 2024.
- The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
- CERT-In Directive No. 20(3)/2022-CERT-In, "Directions under sub-section (6) of section 70B of the Information Technology Act, 2000", April 2022.
- MeitY National Critical Information Infrastructure Protection guidelines, current revision 2024.

International regulations

- Regulation (EU) 2016/679 General Data Protection Regulation.
- Regulation (EU) 2023/2854 on harmonised rules on fair access to and use of data (Data Act).
- People's Republic of China Cybersecurity Law (2017), Data Security Law (2021), Personal Information Protection Law (2021).
- US Clarifying Lawful Overseas Use of Data (CLOUD) Act, 2018.
- Russian Federation Federal Law No. 242-FZ on personal data localisation.

Standards

- ISO/IEC 27001:2022 Information security management.
- ISO/IEC 27017:2015 Cloud services security controls.
- ISO/IEC 27018:2019 Protection of personally identifiable information in public clouds.
- SOC 2 Type II Trust Services Criteria, AICPA 2017 with subsequent amendments.
- NIST SP 800-53 Rev 5 Security and Privacy Controls for Information Systems and Organizations.

HyperNext
Data Centers

HyperNext Research

We publish engineering and policy papers because the Indian conversation about AI infrastructure needs more substance than marketing material provides. The papers state methodology openly so other operators can run the same analysis on their own facilities. They report findings that may not flatter the HyperNext commercial position. They get review from the engineering team and the communications partners.

Correspondence on methods, figures, and conclusions: **hello@hypernxt.com**. We read every email.

HN-RP-003 · India's Sovereign AI Cloud
12 December 2025 · v1.0

www.hypernxt.com/research
hello@hypernxt.com · +91 99784 23333