

Praman Sovereign Compliance for India's Data-Centre Industry

A practical field guide to DPDP (2023) and the CERT-In directions · by Zyvark Solutions

Version 1.0 · 2026-10-11 · praman.zyvark.in · Compliance tooling, not legal advice.

Executive summary

India's data economy is being re-platformed onto domestic, sovereign infrastructure at the exact moment its first comprehensive privacy statute takes force. The Digital Personal Data Protection Act, 2023 (DPDP) and the CERT-In directions of 28 April 2022 together place continuous, evidence-backed obligations on every organisation that processes personal data and a disproportionate share of that weight lands on data-centre and cloud operators, who host the workloads of hundreds of regulated enterprises.

This paper sets out what the law actually requires, why the rise of AI has broken the previous generation of consent-banner tooling, and how Praman delivers continuous, tamper-evident proof of compliance that an operator can hand to its tenants, auditors and cyber-insurers.

1. The regulatory window is now

The DPDP Rules were notified on 13 November 2025, with full compliance expected by 13 May 2027. CERT-In's directions already bind ICT and data-centre operators today. Compliance has shifted from a periodic, document-driven exercise to a continuous, board-level obligation with hard, time-boxed deadlines.

" DPDP: lawful basis and notice for every dataset, purpose and storage limitation, children's-data protections, breach notification to the Data Protection Board and to affected principals.

" CERT-In: reportable cyber incidents within six hours of detection; ICT logs retained 180 days within India; synchronised system clocks.

" Significant Data Fiduciaries: a designated Data Protection Officer, periodic DPIAs, and an annual data audit.

2. Why AI broke the old tools

The previous generation of privacy tooling was built for the web era: cookie consent, subject-access request inboxes, and policy documents. None of it can see the fastest-growing cross-border channel — personal data placed inside a prompt to a foreign large-language-model API. These flows originate deep inside applications and pipelines, are invisible to a consent banner, and in substance constitute a cross-border transfer of personal data.

The risk surface has moved from the browser to the infrastructure and the AI pipeline. Compliance must move with it.

3. The operator's special burden

Data-centre and sovereign-cloud operators carry compliance weight for the enterprises they host. Their tenants increasingly demand in-region proof of residency and handling before they will sign. A compliance tool that is itself hosted on foreign cloud is structurally non-compliant which excludes most incumbent SaaS from the sovereign segment entirely.

- " A single registry of assets, workloads and the flows between them most operators do not have one.
- " Egress to foreign clouds and foreign model APIs classified by jurisdiction and controller.
- " Evidence a tenant, auditor or insurer can trust not screenshots, and not numbers an operator could backdate.

4. What good looks like: continuous, evidence-backed assurance

Praman turns each statutory duty into an automated check with a pass / at-risk / fail status and the citation beside it. Every result is written to an append-only, hash-chained audit log that the database itself refuses to update or delete. A one-click verifier recomputes the chain and pinpoints any tampering, so the exported Audit Pack proves its own integrity.

Watch

Register data centres, clusters, GPU fleets, pipelines and storage. Personal data is classified in-region Aadhaar (with Verhoeff checksum), PAN, phone and email never sent to a foreign API.

Measure

A versioned rule engine evaluates your live state against DPDP and CERT-In obligations. When the law changes, you version the obligation as data no software release required.

Prove

Export a regulator-ready Audit Pack: posture, checks with citations, breach timeline, retention proofs and an integrity certificate, plus the underlying JSON evidence.

5. Sovereign by construction

No component of Praman requires a foreign-hosted service. The entire platform runs in-region with a single `docker compose up`, and the integrity chain verifies clean across every event. Sovereignty is not a deployment option bolted on afterwards it is a property of the design that competitors built on foreign cloud cannot retrofit.

6. A 90-day path to defensible compliance

- " Weeks 1-2: inventory assets, workloads and data flows; import via CSV; classify personal data in-region.

- " Weeks 3-6: load the DPDP + CERT-In obligation library; review and amend with counsel; run the first evaluation.
- " Weeks 7-10: stand up retention clocks, consent records and the breach workflow with its six-hour countdown.
- " Weeks 11-13: export your first Audit Pack; share scoped evidence with a design-partner tenant or your auditor.

Conclusion

The organisations that treat the May 2027 deadline as a continuous-assurance programme rather than a last-quarter document scramble will be the ones their customers, auditors and insurers trust. Praman is the sovereign compliance layer that makes that programme provable.

To arrange a demo or a design-partner conversation: logesh@zyvark.in • praman.zyvark.in

Praman provides compliance tooling, not legal advice. Verify all obligations with qualified counsel.