

A blue circle containing the text "K7" in white.

K7

DPDP Act Readiness Guide for Indian Businesses

3 pages • CyberK7 Whitepaper

A practical roadmap covering consent architecture, data mapping, breach response timelines and DPO readiness for Indian organizations preparing for DPDP Act compliance.

- 1. Why This Matters Now
- 2. The Five Pillars of Readiness
- 3. Common Gaps We Find
- 4. Recommended Next Steps
- About CyberK7

1. Why This Matters Now

The Digital Personal Data Protection Act, 2023 introduced real enforcement teeth to Indian data privacy, with penalties reaching up to ₹250 crore for serious violations. Every organization handling personal data of Indian residents now carries explicit legal obligations.

Unlike previous guidance-based approaches, the DPDP Act empowers the Data Protection Board of India to investigate complaints and levy real financial penalties, making this a board-level risk item.

2. The Five Pillars of Readiness

Data Mapping — know what personal data you collect, where it lives, and who has access. Consent Architecture — consent must be specific, informed, and as easy to withdraw as it was to give. Purpose Limitation — data collected for one purpose cannot silently be repurposed. Breach Response — a documented plan with clear notification timelines is mandatory. Data Protection Officer Readiness — significant data fiduciaries must appoint a DPO.

3. Common Gaps We Find

During assessments, the most frequent gaps are: no central record of personal data across the organization, consent flows that predate the Act, and absence of a tested breach notification process.

4. Recommended Next Steps

Start with a data mapping exercise across all departments. Build or update consent management flows across every collection point. Draft and rehearse a breach response plan. Treat this as an ongoing practice reviewed quarterly.

About CyberK7

CyberK7 is a Delhi-based cybersecurity consulting firm helping organizations build secure, resilient and compliant digital environments through GRC, VAPT, SOC monitoring, cloud security, IAM, EDR/XDR and security awareness training.

To discuss how this applies to your organization, reach us at info@cyberk7.com or +91 98990 62199.

Quick Reference

Readiness Area	Typical Gap Found	Priority
Data Mapping	No central inventory of personal data	High
Consent Flows	Pre-Act consent language still in use	High

Breach Response	No documented 6-hour-ready process	High
DPO Appointment	No designated accountability owner	Medium
Vendor Contracts	Data processing clauses not updated	Medium

For a tailored consultation, contact CyberK7 at info@cyberk7.com or +91 98990 62199.