DPDP Act 2023 and CERT-In Directions: Compliance Essentials for Software Companies

Author: Kamakshaiah Musunuru | **Published:** 11 September 2026 | **Category:** Tech Update | **Read time:** 2 min read

Tags: DPDP Act, data privacy, GDPR, CERT-In, cybersecurity compliance, India

Data protection obligations are no longer optional for software companies operating in India. Two frameworks matter most today: the Digital Personal Data Protection (DPDP) Act 2023 and the CERT-In directions on cyber incident reporting.

The DPDP Act 2023 in Brief

The Act regulates "digital personal data" — data about a person that is processed digitally. Its main themes are consent, purpose limitation and accountability.

- Consent: processing personal data requires free, specific, informed, unconditional and unambiguous consent, with a mechanism to manage and withdraw it - Purpose limitation: data may only be processed for the purpose for which it was collected - Data principal rights: individuals can request access to, correction of and erasure of their data - Significant data fiduciaries: some organisations face additional duties, including a Data Protection Officer and periodic audits - Breach notification: any data breach must be notified to the Board and affected persons without delay

What Templates, Apps and Platforms Must Cover

- A privacy policy that explains what data is collected, why, and how consent can be withdrawn - Consent flows (checkboxes that are not bundled into other terms) with audit trails - A retention and deletion process so data is not kept longer than needed - Technical controls: encryption, access control and logging around personal data - A breach notification runbook

CERT-In Direction on Incident Reporting

CERT-In's directives require service providers and intermediaries to report specified cyber incidents — including data breaches, unauthorised access and ransomware — within six hours of detection (for certain categories) through the CERT-In portal. Timely detection capability is therefore not optional; you must be able to detect and report.

Interplay with Other Regimes

If you also handle European data, the GDPR applies in parallel, and many enterprises ask for ISO 27001 or similar certifications from their vendors. A single, well-built privacy programme usually covers DPDP, GDPR basics and ISO 27001 readiness together.

Codingfigs helps software companies design privacy-compliant products — consent flows, privacy policies, DPIA, and compliance audits aligned with DPDP, GDPR and ISO 27001. To discuss your obligations, reach out to our compliance practice.