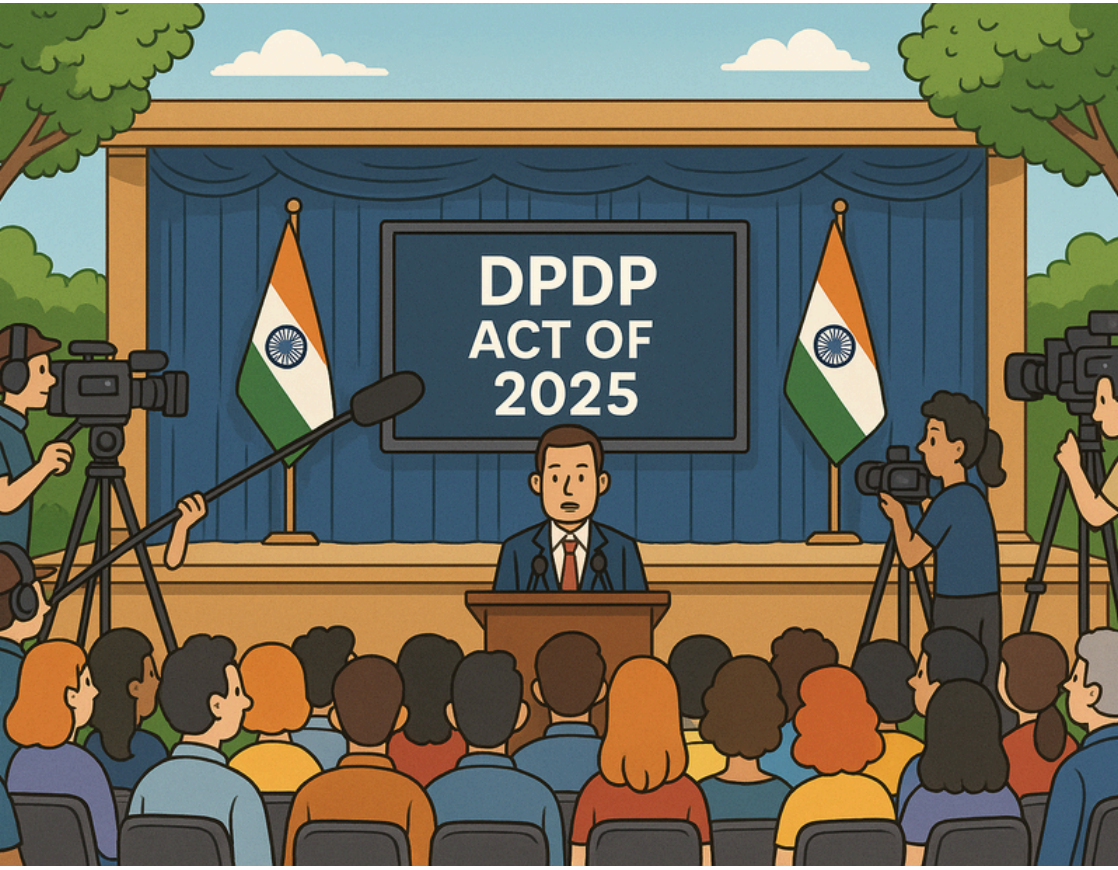
DPO ASSOCIATION



DPDP REGULATORY COMPLIANCE GUIDE 2025

Site no. 192, 13th cross,
Jayasuryanagar, Jakkur post,
Bengaluru, Karnataka, ,
India - 560064

+91 9845568869

info@dpoassociation.org

www.dpoassociation.org

Introduction & Background

The DPDP Act, 2023 provides a legal framework to protect the privacy and personal data of individuals in India. As digital data grows across systems, organizations must ensure responsible and compliant handling of personal information.
The DPO Association is committed to implementing strong governance, procedures, and employee responsibilities under the Act. This handbook supports employees, contractors, and third-party vendors by outlining the data protection framework for audits, management reviews, and regulatory inspections.

Significance of the DPDP Act

The Act safeguards individuals' personal data and ensures their privacy rights are respected. It defines legal obligations for organizations processing personal data and strengthens trust among customers, employees, and stakeholders.
It also provides a risk management framework for preventing misuse, breaches, and unauthorized processing, while aligning India with global data protection standards.

Key Goals of the DPDP Compliance Program

The Act promotes lawful, fair, and transparent processing of personal data while defining rights of individuals and responsibilities of organizations. It establishes accountability through governance, audits, and security safeguards.
The program also ensures grievance redressal, breach reporting, and encourages trust in digital services and data-driven operations.

Applicability Framework

The DPDP Act applies to all organizations that determine how personal data is processed, and to third-party processors acting on their behalf. It covers all digital personal data of employees, customers, vendors, and partners.
The Act applies to processing within India and cross-border transfers, except for specific exemptions related to government functions, national security, and law enforcement.

Essential Elements of the DPDP Act

Data Principal	The data owner or the subject of the personal data.
Data Fiduciary	The controller that governs data processing activities.
Data Processor	An agent or vendor performing processing as instructed.
Personal Data	Information that can directly or indirectly identify an individual.
Consent	Requires clear, voluntary, informed agreement with no ambiguity

Data Principal Rights Framework

Duties and Responsibilities of Individuals

- Share accurate and updated personal data.
- Submit requests responsibly without any misuse.
- Keep login details safe from others.
- Report suspected data misuse immediately.
- Understand and withdraw consent when needed.

Core Obligations of Data Controllers

Data fiduciaries (organizations controlling data processing) are mandated to uphold specific obligations:

- Ensure lawful and transparent data processing.
- Collect and manage consent effectively.
- Protect personal data with strong security.
- Maintain records to demonstrate compliance.
- Provide a system for grievance handling.
- Collect minimal data for defined purposes.

Special Requirements for Minors' Data

- Obtain verifiable parental or guardian consent.
- Clearly explain data use to children.
- Collect only necessary child-related data.
- Apply stronger security for children's data.
- Review compliance practices regularly for minors.

High-Risk Data Fiduciaries

Appoint a qualified DPO within India.

Conduct annual independent compliance audits.

Perform DPIAs for high-risk processing.

Implement strong security and governance controls.

Enforcement and Penalty Framework

Non-compliance with DPDP obligations may result in significant penalties and corrective measures. Key examples include:

Up to ₹250 Crore	Failure to prevent a data breach.
Up to ₹200 Crore	Violation of obligations involving children's data.
Up to ₹200 Crore	Failure to comply with consent and notice requirements.
Up to ₹50 Crore	Failure to correct or erase personal data.

DPDP 2025 – Implementation & Operational Controls

Notice Requirements

Privacy notices must be clear, bilingual, and purpose-specific. They should explain data collection, retention, cross-border transfers, and Data Principals' rights. Providing clarity reduces compliance risk.

Rule 03

Rule 04

Consent Managers

Consent Managers must be registered, neutral, and independent. They handle consent access, withdrawal, and history with bilingual interfaces. Real-time logs enhance transparency.

Security Safeguards

Implement RBAC, MFA, and encryption across systems. Regularly log and monitor access events. Conduct annual audits to review security controls.

Rule 06

Rule 07

Breach Notification

Maintain a breach response plan with escalation tiers. Report breaches within 72 hours and keep a live breach register. Document mitigation and corrective actions.

Retention & Erasure

Define retention timelines and automate erasure once objectives are met. Maintain logs of deletions for audit readiness and policy compliance.

Rule 08

DPDP 2025 – Implementation & Operational Controls

Rule 10

Processing of Children's Data
Verify age and obtain parental consent before processing. Disable profiling or tracking for minors. Ensure all systems comply with children's data protections.

Obligations of Significant Data Fiduciaries
Enable centralised rights portals for access, correction, and erasure requests. Maintain SLA compliance and ensure timely handling of all requests.

Rule 13

Rule 14

Rights of Data Principals
Provide easy mechanisms for Data Principals to exercise rights. Use RBAC, MFA, logging, and encryption to protect these operations. Review processes annually.

Cross-Border Transfers
Apply DPDP clauses in contracts and track all cross-border data flows. Maintain geo-transfer logs, limit access to authorized teams, and validate data integrity regularly.

Rule 15

DPDP 2025 – Regulatory Timelines & Milestones

Immediate Priorities (0–3 Months)

- Appoint a Grievance Officer.
- Publish a bilingual, purpose-specific privacy notice.
- Activate consent collection and withdrawal mechanisms.
- Map all personal data processing activities.
- Establish breach reporting processes and minimum safeguards.

Short-Term Milestones (3–6 Months)

- Finalize governance policies and operational procedures.
- Update contracts with processors and partners.
- Implement consent manager integration where applicable.
- Strengthen logging, monitoring, and access controls.

Medium-Term Actions (6–12 Months)

- Complete end-to-end data flow and lifecycle mapping.
- Conduct risk assessments and DPIA where required.
- Implement automated inactivity-based data deletion.
- Validate compliance readiness through internal reviews.

Annual & Ongoing Obligations

- Conduct annual audits and DPIAs (for SDFs).
- Refresh policies, controls, and contractual clauses.
- Provide regular staff training and awareness programs.
- Continuously monitor systems and update privacy notices as needed.

GOVERNANCE

1. Appoint a DPO/Grievance Officer and define roles clearly.
2. Establish DPDP governance policies and accountability structures.
3. Maintain compliance documentation, logs, and audit trails.
4. Conduct annual audits and periodic compliance reviews.

NOTICES & CONSENT

1. Publish clear, bilingual privacy notices with purpose, retention, rights, and grievance details.
2. Implement consent collection, withdrawal, and tracking mechanisms.
3. Maintain auditable consent logs and ensure transparency.
4. Use registered Consent Managers wherever applicable.

SECURITY CONTROLS

1. Enforce MFA, RBAC, and strong access controls.
2. Encrypt data at rest and in transit.
3. Maintain logging, monitoring, and anomaly detection systems.
4. Review security controls annually and update as needed.

BREACH MANAGEMENT

1. Establish a breach response plan with defined escalation levels.
2. Provide immediate breach notification and a full report within 72 hours.
3. Maintain a breach register with root-cause analysis and corrective actions.
4. Train teams regularly on breach-handling procedures.

DPDP 2025 – Consolidated Checklist

RETENTION & ERASURE

1. Define purpose-based retention periods for all personal data.
2. Enable automated deletion once the purpose is fulfilled or consent withdrawn.
3. Maintain deletion logs for audit readiness.
4. Apply data minimization principles across systems

CHILDREN'S DATA

1. Obtain verifiable parental/guardian consent before processing.
2. Disable tracking, profiling, or targeted advertising for minors.
3. Apply enhanced technical and organizational safeguards.
4. Review children's data processing practices regularly.

DATA PRINCIPAL RIGHTS

1. Provide mechanisms for access, correction, and erasure requests.
2. Respond to rights requests within the mandated SLA (90 days).
3. Maintain request logs and ensure transparent communication.
4. Enable nomination rights for incapacitation or death.

CROSS-BORDER TRANSFERS

1. Allow transfers only to permitted countries or under allowed conditions.
2. Maintain logs of all cross-border data flows.
3. Ensure contractual safeguards with processors and partners.
4. Continuously monitor compliance with transfer requirements.

About DPO Association

The DPO Association is a professional body dedicated to empowering Data Protection Officers and privacy practitioners across India.
We provide guidance, resources, and expert support to help organizations navigate the evolving regulatory landscape with confidence.
Our focus areas include DPDP compliance, privacy governance, risk management, and capacity-building for data protection professionals.
Through structured frameworks and industry collaboration, we promote responsible data handling, accountability, and sustainable governance practices.

Audit & Assessment

1. Expert-led privacy and data protection audits for organizations and DPO teams.
2. Identify compliance gaps, maturity levels, and operational risks.

Compliance Roadmaps

1. Develop tailored DPDP implementation roadmaps for organizations of all sizes.
2. Define clear milestones, timelines, and responsibilities for full compliance.

Process Integration

1. Support integrating privacy by design into policies, processes, and technology systems.
2. Enable DPOs to embed governance practices into day-to-day operations.

Capacity Building & Ongoing Support

1. Capacity Building & Ongoing Support
2. Continuous training, workshops, and knowledge sessions for DPOs and privacy teams.
3. Regular regulatory updates, advisory notes, and compliance guidance.

Join Us to Strengthen India's Data Protection Ecosystem

Discover how the DPO Association can support your organization in achieving structured, scalable, and future-ready DPDP compliance.

Schedule a one-hour knowledge-sharing session with our privacy experts and take the first step toward strengthened governance and accountability.

Empowering DPOs. Advancing Privacy. Protecting Trust.

DPO Association of India

www.dpoassociation.org