Telecom & Internet Service Providers

DPDPA 2023 Implementation Handbook

Digital Personal Data Protection Act, 2023 • India

For mobile operators, broadband ISPs, OTT communication apps, and satellite internet providers.

1. Overview & Applicability

Telecom operators and ISPs sit at the infrastructure layer of the internet — processing call records, location data, browsing activity, and subscriber profiles at massive scale. They are subject to both the DPDPA and sector-specific regulations under the Telecom Regulatory Authority of India (TRAI) and the Telegraph Act. Large operators are almost certain to be designated as Significant Data Fiduciaries, triggering additional obligations including mandatory DPO appointment.

2. Key Definitions Under DPDPA

These definitions govern how the Act applies to your sector:

Call Detail Records (CDRs)	Records of calls made, received, duration, and location — personal data of subscribers.
Location Data	Real-time or historical location derived from cell towers or GPS — highly sensitive.
Subscriber Data	Name, address, identity documents, payment details provided at SIM activation — core personal data.
Browsing Data	URLs visited, data usage patterns — personal data when linked to a subscriber.
Lawful Interception	Government-authorised interception is a legitimate use under the Telegraph Act — document each instance.
SDF Status	Telecom operators with large subscriber bases are likely to be designated SDFs.

3. Core Compliance Obligations

Every entity in this sector that processes personal data must comply with the following obligations:

1	**Subscriber Consent Management** Separate consent is required for marketing, analytics, and profiling beyond billing. The initial subscription agreement does not cover these uses.
2	**Location Data Governance** Location data must never be sold to third parties without explicit subscriber consent. Real-time location access by apps requires affirmative opt-in.
3	**CDR Retention & Access** CDRs must be retained only for the period required by law. Access must be restricted to authorised personnel with audit logs.
4	**Data Breach Notification** Telecom networks are high-value targets. Implement a 24/7 breach monitoring system and DPBI notification protocol.
5	**Third-Party Data Sharing** Do not share subscriber data with advertisers, data brokers, or analytics companies without explicit consent and a DPA.
6	**OTT Communication Apps** Apps using telecom infrastructure (WhatsApp, Zoom) must ensure message metadata is not processed beyond service delivery without consent.
7	**SDF Obligations** Appoint an India-based DPO. Conduct annual data audits. Perform DPIAs before launching new data-intensive services.

4. Implementation Checklist

Use this checklist to track your DPDPA compliance readiness:

- ☐ Audit all subscriber data stores — CDRs, location databases, payment records, ID documents.
- ☐ Separate marketing consent from service delivery consent in all SIM activation and app onboarding flows.
- ☐ Implement strict access controls on CDRs — only authorised teams with audit trails.
- ☐ Review all data-sharing agreements with advertisers, analytics partners, and government agencies.
- ☐ Implement a 24/7 network security monitoring and breach detection system.
- ☐ Build a subscriber rights portal — access, correction, erasure, and grievance request flows.
- ☐ Execute DPAs with all third-party data processors (billing vendors, analytics platforms, cloud providers).
- ☐ Appoint an India-based DPO (if SDF) and publish DPO contact details.
- ☐ Conduct a DPIA before launching any new location-based service, targeted advertising product, or AI feature.
- ☐ Train customer service, network operations, and IT security teams on DPDPA obligations.
- ☐ Review cross-border data sharing with international roaming partners and submarine cable operators.

5. Applicable Penalties

The Data Protection Board of India (DPBI) may impose the following penalties for non-compliance:

Rs. 250 Crore	Failure to implement reasonable security safeguards resulting in a personal data breach
Rs. 200 Crore	Breach of obligations related to processing children's personal data
Rs. 150 Crore	Failure to fulfill obligations as a Significant Data Fiduciary (SDF)
Rs. 50 Crore	Failure to comply with Data Principal rights or other provisions of the Act

6. Implementation Roadmap

Follow this phased approach to achieve full DPDPA compliance:

1	**Month 1: Regulatory Alignment** Map DPDPA obligations against TRAI regulations and Telegraph Act requirements.
2	**Month 2: Subscriber Data Audit** Catalogue all personal data — CDRs, location, subscriber profiles, payment records.
3	**Month 3: Consent Infrastructure** Build granular consent management integrated into your CRM and subscriber portal.
4	**Month 4: Security Uplift** Enhance CDR access controls, implement breach detection, and test incident response.
5	**Month 5: DPO & Audit Prep** Appoint DPO, initiate first independent data audit, build DPIA framework.
6	**Month 6+: Ongoing** Quarterly subscriber data reviews, annual TRAI-DPDPA compliance assessments.

🛡️ Telecom data is among the most valuable and sensitive. Location data and CDRs, if breached, constitute a serious violation. Invest in network-level data security as a priority.