Kredo Analytics

DIGITAL PERSONAL DATA PROTECTION ACT, 2023 · DPDP RULES, 2025

DPDP Act, 2023 Industry-wise Implementation Guidelines

Practical sector-by-sector compliance guide for Indian enterprises

COVERING 12 INDUSTRY SECTORS

Banking & Financial Services · Healthcare · IT/SaaS · E-Commerce · Telecom · HR/Staffing · Education · Real Estate · Professional Services · Manufacturing/Supply Chain · Media & Digital Platforms · Government & PSUs

PREPARED BY

Kredo Analytics Private Limited
Chartered Accountants, lawyers and engineers on one team
Bengaluru, India · Monroeville, PA, USA
ISO/IEC 27001:2022 certified

SECTION A

How to use this guide

This document translates the Digital Personal Data Protection Act, 2023 and the DPDP Rules, 2025 into actionable, sector-specific implementation programmes. While the Act is sector-agnostic in its legal obligations, its practical impact varies significantly across industries — the type of personal data processed, the volume, the sensitivity, the presence of children's data, the cross-border flows, and the regulatory overlap with existing sectoral laws all differ materially.

Each industry section is structured as follows:

- **Data Landscape** — the categories of personal data commonly processed
- **Key DPDP Risks** — the pressure points specific to that sector
- **Implementation Steps** — a sequenced action plan
- **Sector-Specific Special Obligations** — where the DPDP intersects with existing sectoral regulation
- **Penalty Exposure** — the financial risk profile
- **Compliance Checklist** — ready-to-use action items with priority and timing

Compliance timeline. Full substantive compliance (consent, notice, breach notification, Data Principal rights, penalties) is required by 13 May 2027. MeitY consultations in January 2026 proposed accelerating this to November 2026 — treat that as the prudent target.

Common foundation — applicable to all industries

Regardless of sector, every Data Fiduciary must complete the following universal baseline before addressing sector-specific requirements:

FOUNDATION ELEMENT	WHAT IT REQUIRES
Data Inventory & Mapping	Catalogue every category of personal data, its source, storage location, processing purpose, and who it is shared with (Data Processors, third parties, overseas entities).
Record of Processing Activities (RoPA)	A living document recording: data categories, lawful basis, purpose, retention period, recipients, and cross-border transfer details for each processing activity.
Consent Architecture	Replace all bundled/implied consents with free, specific, informed, opt-in consent. Build withdrawal mechanisms as simple as the consent flow.
Privacy Notice	Standalone notice in plain language, available in English + relevant 8th Schedule languages. Covers: data collected, purpose, rights, complaint route to Board.
Grievance Redressal	Published contact point (or DPO for SDFs). Resolve all complaints within 90 days. Build an escalation path to the Data Protection Board.
Security Safeguards	Encryption at rest and in transit; access controls (least privilege); audit logs retained for at least 1 year; vulnerability management; secure SDLC.
Breach Response Plan	Detection, internal escalation, Board notification (72 hours), individual notification (without delay). All breaches notifiable — no de minimis threshold.
Processor Contracts	All third-party data processors must be under written contracts that are DPDP-aligned: processing scope, security obligations, breach notification, sub-processor controls, and deletion on termination.
Retention & Deletion	Data deleted once purpose is served or consent withdrawn. For sectors with statutory retention requirements, document the legal basis for continued retention.
Children's Data Controls	Age verification; verifiable parental consent; no behavioural monitoring or targeted advertising directed at minors (under 18).

SECTOR 01 OF 12

1. Banking, Financial Services & Insurance (BFSI)

Highest data sensitivity exposure | Overlaps with RBI, SEBI, IRDAI, PMLA regulations | Likely SDF candidates

Data landscape — what personal data is processed

- PAN, Aadhaar, passport, voter ID — identity documentation
- Bank account numbers, IFSC, credit/debit card details, UPI handles
- Credit scores, loan repayment history, income and asset details
- Insurance policy details, health disclosures, nominee information
- KYC documents, VKYC recordings, selfies with liveness checks
- Transaction records, SMS alerts, push notifications, login OTPs
- Investment portfolios, trading history, demat account details
- Signatures (digital and scanned), biometric authentication logs

Key DPDP risks & regulatory pressure points

- **SDF designation risk** — banks, insurance companies, NBFCs, and payment aggregators processing data of crores of Indians are primary SDF candidates. Designation would trigger DPO appointment, DPIAs, independent data audits, and potential data localisation.
- **Overlapping regulatory regimes** — RBI's Master Directions on IT (2021), SEBI's Cyber Security Framework, IRDAI data protection guidelines, and PMLA retention obligations all operate alongside the DPDP Act. Data retained for AML/KYC compliance under PMLA (5–10 years) is a legitimate retention basis under Section 7 — but must be documented.
- **Consent complexity** — CKYC data shared across the financial system means a single customer's consent withdrawal has cascading implications for multiple downstream users of that data.
- **Breach risk and cost** — financial data breaches are among the most damaging — ₹250 crore maximum penalty plus reputational damage, regulatory sanctions, and SEBI/RBI enforcement exposure.
- **Cross-border** — payment processing, correspondent banking, and investment banking workflows regularly involve overseas data transfer. Current negative-list approach is permissive but must be tracked.
- **Fraud investigation carve-out** — investigations of defaulting borrowers and fraud claims fall under the legitimate use exemption (recovery of financial obligations) — document carefully.

Implementation steps — sequenced action plan

- **Data Mapping** — Map all personal data across CBS, CRM, treasury, mobile banking, VKYC, and analytics systems. Identify data shared with credit bureaus, insurance repositories (IIB), depositories (CDSL/NSDL), and payment networks.
- **Legal Basis Rationalisation** — PMLA, KYC Master Directions, and RBI guidelines provide legitimate use bases for most core processing. Document each processing activity against its DPDP lawful basis — avoid defaulting to consent for activities already covered by legal obligation.
- **Consent Rebuild** — Marketing, cross-sell, analytics, and non-mandatory communications must be restructured on fresh DPDP-compliant consent. Decouple product consent from marketing consent.
- **VKYC and Biometrics** — VKYC recordings, liveness selfies, and voice records are processed on consent — review the granularity and retention. Implement auto-deletion workflows post-KYC verification.
- **Processor Governance** — Re-paper all fintech partnerships, BPO/outsourcing contracts, and cloud vendor agreements with DPDP clauses. Review sub-processor chains (e.g., bureau → bank → analytics vendor).
- **Breach Protocol** — Financial institutions already have RBI incident reporting frameworks — integrate DPDP breach notification (72 hours to Board + individual notification) into existing CISO/incident response SOPs.
- **SDF Readiness** — Large banks and insurance companies should begin DPO search and DPIA methodology development now — SDF notifications are expected once the Board is fully operational.
- **Customer Portal** — Build a self-service rights portal allowing customers to exercise access, correction, erasure, nomination, and consent withdrawal rights within 90-day timelines.

Sector-specific special obligations

- RBI Master Direction on IT Framework (2021) requires a Data Governance Framework — align this with DPDP RoPA and security safeguard requirements.
- SEBI Cyber Security & Cyber Resilience Framework (2023): already requires breach reporting — integrate with DPDP 72-hour Board notification obligation.
- IRDAI data protection provisions under Insurance Act and IRDAI (Protection of Policyholders) Regulations: policyholder data retention must be reconciled with DPDP purpose-limitation rules.
- PMLA: customer data retained for AML compliance (5–10 years) is permissible under the DPDP Act's legal-obligation legitimate use — must be explicitly documented.
- Account Aggregator (AA) framework: AAs are Consent Managers in the DPDP ecosystem. Banks as Financial Information Providers (FIPs) and Users (FIUs) must ensure AA consent flows meet DPDP standards.
- Credit Bureaus (CIBIL, Experian, CRIF, Equifax): data sharing must be under DPDP-aligned agreements. Individuals have a right to correction — build a bureau dispute escalation workflow.

PENALTY EXPOSURE	Maximum ₹250 crore for security failures + ₹200 crore for breach non-notification. As likely SDFs, large BFSI entities also face ₹150 crore for SDF obligation breaches. The Board's financial-sector expertise from SEBI/IRDAI panel members is expected to drive early enforcement in this sector.

Compliance checklist

ACTION ITEM	PRIORITY	TARGET
Complete cross-system data inventory (CBS, CRM, mobile, VKYC, analytics)	CRITICAL	Month 1–2
Document lawful basis for each processing activity against DPDP/PMLA/RBI	CRITICAL	Month 2–3
Redesign marketing consent — decouple from product onboarding	CRITICAL	Month 3–4
Re-paper fintech, BPO, and analytics processor contracts	CRITICAL	Month 3–5
Integrate DPDP breach notification into CISO SOPs	HIGH	Month 4
Build customer rights portal (access, correction, erasure, nomination)	HIGH	Month 5–8
VKYC recording retention policy — auto-deletion post-verification	HIGH	Month 4–5
Begin SDF readiness programme (DPO search, DPIA framework)	HIGH	Month 6–9
Staff training — front-line, ops, IT, compliance, legal	MEDIUM	Month 4–6
Align with RBI IT Framework, SEBI CSCRF, IRDAI guidelines	MEDIUM	Ongoing

SECTOR 02 OF 12

2. Healthcare & Pharmaceuticals

Highly sensitive personal data | Unique patient confidentiality obligations | No 'sensitive data' category in DPDP — but health data processed under breach-risk scrutiny

Data landscape — what personal data is processed

- Patient name, age, contact details, Aadhaar/insurance ID
- Diagnosis, prescription, treatment history, discharge summaries
- Pathology reports, radiology images, genetic test results
- Mental health records, addiction treatment history
- Insurance claim records, TPA data, pre-authorisation documents
- Video consultation recordings (telemedicine)
- Pharmacy purchase history, medicine delivery addresses
- Clinical trial participant data, adverse event reports
- Employee health records (pre-employment, periodic medicals)

Key DPDP risks & regulatory pressure points

- **No explicit 'sensitive data' tier** — Unlike GDPR which grants special protection to health data, the DPDP Act treats all personal data uniformly. However, health data breaches are likely to attract maximum penalties given their potential harm — the Board will apply proportionality.
- **Medical emergency exemption** — processing without consent is permitted in medical emergencies involving threat to life (Section 7). Hospitals must document their protocols for invoking this exemption precisely.
- **Telemedicine** — DPDP consent obligations apply directly to telemedicine platforms, which record consultations and process prescriptions. Platforms must issue DPDP-compliant consent notices at registration and before each consultation.
- **Minors** — patients under 18 require verifiable parental consent — paediatric hospitals, vaccination platforms, and school health programmes must implement age-gating.
- **Pharmaceutical clinical trials** — participants are Data Principals. Clinical trial data processing is heavily regulated by CDSCO/ICMR — overlay DPDP consent requirements on top of informed consent forms.
- **Third-party insurance and TPA sharing** — health data shared with insurance companies and TPAs for claims processing must be under DPDP-aligned processor agreements.

Implementation steps — sequenced action plan

- **Data Inventory** — Map all patient data flows: intake forms → EMR/HIS → labs → pharmacy → insurance → discharge → follow-up. Identify telemedicine platforms, diagnostic integrations, and cloud storage.
- **Consent Rebuild** — Current consent forms under MCI/NMC Guidelines and Clinical Establishments Act do not meet DPDP standards. Update patient intake consent forms to be DPDP-compliant — separate medical treatment consent from data processing consent.
- **Purpose Limitation** — Health data collected for treatment cannot be repurposed for pharma marketing, research, or AI model training without fresh, specific consent. Audit all secondary uses.
- **Telemedicine Compliance** — Align with Telemedicine Practice Guidelines (2020) + DPDP: consent notices at app sign-up, recording retention policies, secure video infrastructure, and breach detection.
- **TPA and Insurer Contracts** — Re-paper all TPA and health insurer data-sharing agreements with DPDP processor clauses.
- **Employee Health Data** — Health data collected for pre-employment medicals or workplace safety is processed under employment legitimate use — but must be proportionate and deleted when no longer needed.
- **Data Security Upgrade** — Healthcare is a high-value breach target. Implement end-to-end encryption for EMR data, role-based access for clinicians vs. billing vs. admin staff, and secure APIs for lab integrations.
- **Grievance Mechanism** — Publish a patient data grievance officer contact. Hospitals should integrate this into patient admission and discharge paperwork.

Sector-specific special obligations

- Clinical Establishments (Registration and Regulation) Act, 2010: patient records retention requirements must be reconciled with DPDP's deletion obligations — legal retention obligation is a valid basis for extended retention.
- ICMR National Ethical Guidelines for Biomedical Research (2017): informed consent for research — ensure DPDP consent requirements are reflected in IRB/IEC-approved consent forms.
- Telemedicine Practice Guidelines (2020): patient data confidentiality obligations — directly compatible with DPDP, but consent formalities need upgrading.
- CDSCO/Schedule Y: clinical trial data — DPDP consent applies to trial participants in addition to regulatory requirements.
- IT Act, 2000 and SPDI Rules, 2011 (until replaced): health/medical records are Sensitive Personal Data under current SPDI Rules — DPDP Act will supersede, but interim compliance must be maintained.

PENALTY EXPOSURE	Breach of patient health data — up to ₹250 crore for security failures. Hospitals processing data of large patient populations are also at SDF designation risk once thresholds are defined.

Compliance checklist

ACTION ITEM	PRIORITY	TARGET
Update patient intake consent forms (DPDP-compliant, separate from medical consent)	CRITICAL	Month 1–3
Audit all secondary uses of patient data (marketing, research, AI)	CRITICAL	Month 2–3
Re-paper TPA and insurer data-sharing agreements	CRITICAL	Month 3–5
Implement end-to-end EMR encryption and role-based access	CRITICAL	Month 2–6
Telemedicine platform: DPDP consent at sign-up + recording retention policy	HIGH	Month 3–5
Minor patients: age-gating and verifiable parental consent	HIGH	Month 4–6
Employee health data: proportionality review and deletion schedule	MEDIUM	Month 4–5
Build patient data grievance redressal mechanism	HIGH	Month 4–6
Align clinical trial consent forms with DPDP + ICMR guidelines	MEDIUM	Month 5–8
Data breach response drill including Board notification (72 hr)	HIGH	Month 6

SECTOR 03 OF 12

3. Information Technology, SaaS & Technology Companies

Dual role: Data Fiduciary for employees/users AND Data Processor for enterprise clients | Export of data processing services — extra-territorial exposure | High SDF risk for large platforms

Data landscape — what personal data is processed

- End-user/consumer account data: name, email, phone, device ID
- Behavioral data: clickstream, session logs, search history, feature usage
- Employee data: HR records, payroll, performance, background checks
- Client data processed under BPO/outsourcing contracts
- Authentication data: usernames, hashed passwords, MFA logs, biometric logins
- Support tickets, chat logs, screen-share recordings
- Usage analytics, A/B testing data, cohort analysis
- Marketing databases: lead lists, email lists, campaign response data

Key DPDP risks & regulatory pressure points

- **Dual Fiduciary/Processor role** — For enterprise SaaS, the company is typically a Data Processor (client is the Fiduciary) — but for direct consumer products, it is a Data Fiduciary. Contractual protections flow in one direction; regulatory liability flows in the other. This must be clearly mapped for each product.
- **Extra-territorial scope** — any SaaS product with Indian users — even hosted globally — is subject to the DPDP Act for those users. US-based parent entities of Indian SaaS companies face Indian compliance obligations.
- **Consent Manager opportunity** — technology companies are well-positioned to register as Consent Managers (from November 2026) — a significant business opportunity in the DPDP compliance ecosystem.
- **Employee data** — IT companies employ hundreds of thousands of professionals. Employee data processing for background verification, access management, payroll, and performance is covered under employment legitimate use — but the scope must be proportionate.
- **AI/ML model training** — training AI models on user data requires a specific, separate consent — repurposing behavioral analytics data for model training without fresh consent is a significant violation risk.
- **Data minimisation pressure** — IT companies historically collect broad analytics data. The DPDP Act's data minimisation principle will require re-engineering of analytics pipelines to collect only what is necessary.

Implementation steps — sequenced action plan

- **Role Classification** — For each product/service, determine the role: Data Fiduciary (consumer products, HR systems) vs. Data Processor (enterprise SaaS). This determines where legal accountability sits.
- **Enterprise Contract Review** — Review all Data Processing Agreements (DPAs) with enterprise clients. Ensure DPDP-aligned DPA templates are in place covering: processing scope, security, breach notification, sub-processor controls, data return/deletion on termination.
- **Consumer Consent Architecture** — Redesign in-product consent flows: granular, purpose-specific, opt-in. Separate core product consent from analytics, marketing, and AI training consent.
- **Privacy by Design** — Embed DPDP compliance into the SDLC: privacy impact assessments at product design stage, data minimisation in feature specifications, secure coding standards, and automated data retention/deletion.
- **AI/ML Governance** — Audit all data used for AI/ML model training. Obtain specific consent for AI training use-cases. Document model training data provenance. For SDFs, algorithmic transparency requirements will apply.
- **Employee Data Programme** — Map all HR data processing — recruitment, onboarding, access management, payroll, performance, exit. Document the legitimate use basis. Update employment agreements and HR privacy notices.
- **Breach Detection & Response** — Implement SIEM/SOAR tools with DPDP-aligned breach classification and notification workflows. 72-hour Board notification + individual notification — automate where possible.
- **Security Certifications Alignment** — ISO 27001/SOC 2 certifications already cover much of Section 8's security safeguard requirements. Gap-map and use existing audit frameworks to demonstrate DPDP compliance.

Sector-specific special obligations

- CERT-In Directions (April 2022): mandatory breach reporting to CERT-In within 6 hours — integrate with DPDP 72-hour Board notification (two parallel obligations, different timelines).
- NASSCOM / MeitY Data Localisation: for SDFs, potential data localisation requirements. GCCs and captive units of foreign companies must track localisation directions carefully.
- MeitY's IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021: significant social media intermediaries have existing due-diligence and grievance redressal obligations — align with DPDP.
- IT Act Section 43A replacement: the SPDI Rules are superseded by the DPDP Act — migrate all compliance programme references from SPDI to DPDP.
- Cross-border data transfers for IT services: service delivery to US, EU, and APAC clients involves regular data export — maintain a transfer register. EU client contracts already have GDPR DPA requirements; ensure they cover DPDP obligations for Indian employee/user data.

PENALTY EXPOSURE	SaaS platforms with large Indian user bases face ₹250 crore security breach exposure. AI companies using personal data for model training without consent face significant penalty risk. Large platforms will likely be among the first SDF designees.

Compliance checklist

ACTION ITEM	PRIORITY	TARGET
Map Fiduciary vs. Processor role for each product/business line	CRITICAL	Month 1
Update enterprise DPA templates with DPDP-aligned clauses	CRITICAL	Month 2–4
Redesign consumer consent: granular, purpose-specific, opt-in	CRITICAL	Month 3–5
Audit AI/ML training data — obtain fresh consent for AI use-cases	CRITICAL	Month 3–5
Integrate DPDP breach notification into SIEM/incident response SOPs	CRITICAL	Month 3–4
Gap-map ISO 27001/SOC 2 controls against DPDP Section 8 requirements	HIGH	Month 2–3
Embed privacy-by-design into SDLC (PIA at design stage)	HIGH	Month 4–6
Map all employee data — document employment legitimate use basis	HIGH	Month 3–4
Align CERT-In breach reporting with DPDP 72-hour obligation	HIGH	Month 2–3
Assess Consent Manager registration opportunity (from Nov 2026)	MEDIUM	Month 8–10

SECTOR 04 OF 12

4. E-Commerce & Retail

High data volume — likely SDF candidates | Consumer-facing consent complexity | Personalisation vs. privacy tension | Children's data significant risk

Data landscape — what personal data is processed

- Customer profile: name, email, mobile, delivery addresses, date of birth
- Payment data: card details (tokenised), UPI IDs, wallet balances
- Purchase history, wishlist, cart data, return/refund records
- Behavioural data: browsing patterns, clickstream, time-on-page
- Device identifiers, IP addresses, location data (for delivery)
- Customer reviews, ratings, social login data
- Loyalty programme data, referral chains
- Customer service chat logs, complaint records
- Demographic profiles for personalisation and recommendation engines

Key DPDP risks & regulatory pressure points

- **SDF designation certainty** — e-commerce platforms with 2 crore+ users are explicitly referenced in the Third Schedule (default 3-year retention from last login/transaction) — implying SDF designation is expected for large players.
- **Personalisation engine conflict** — recommendation algorithms, retargeting ads, and dynamic pricing use behavioral data that was historically collected under broad, bundled consent. DPDP requires specific consent for each use case.
- **Children** — young shoppers (under 18) are common on e-commerce platforms. Age verification at account creation and verifiable parental consent for minors is mandatory — no targeted advertising to children.
- **Third-party seller data sharing** — customer order data shared with marketplace sellers constitutes a data transfer — sellers need to be classified as Data Processors or separate Data Fiduciaries, with appropriate contracts.
- **Dark patterns** — consent obtained through pre-ticked boxes, misleading UI, or consent fatigue is invalid under the Act. DPDP-era UI design must meet affirmative opt-in standards.
- **Return and refund data** — reason for returns, dispute data, and fraud flags associated with individuals constitute personal data and must be handled within the DPDP framework.

Implementation steps — sequenced action plan

- **Customer Consent Overhaul** — Redesign checkout and account creation flows. Separate: (a) order fulfillment consent (can rely on contractual basis), (b) marketing consent (opt-in), (c) personalisation/analytics consent (opt-in), (d) third-party sharing consent (opt-in).
- **Age Verification** — Implement age verification at account creation. For identified minor accounts, gate targeted advertising, behavioral tracking, and certain product categories. Obtain verifiable parental consent.
- **Seller/Partner Governance** — Classify marketplace sellers as Data Processors (if processing customer data on your instructions) or separate Fiduciaries (if making independent processing decisions). Execute appropriate contracts.
- **Recommendation Engine Audit** — Map all data inputs to personalisation and recommendation algorithms. Obtain specific consent for personalisation use. Build opt-out mechanisms that still allow basic shopping functionality.
- **Retention Schedules** — The Third Schedule prescribes 3-year default retention for e-commerce platforms with 2 crore+ users from last login/transaction. Implement automated deletion workflows.
- **Delivery Partner Management** — Delivery addresses and order details shared with logistics partners must be under DPDP processor agreements. Restrict sharing to minimum necessary.
- **Breach Protocol** — E-commerce breach (payment data, address data) affects large numbers — plan for mass individual notification capability and Board reporting within 72 hours.
- **Rights Portal** — Build a self-service My Data dashboard: view what data is held, correct name/address, request deletion of account, withdraw marketing consent — all resolvable within 90 days.

Sector-specific special obligations

- Consumer Protection (E-Commerce) Rules, 2020: display seller information, grievance officer details, and return policy — align grievance officer with DPDP grievance contact.
- RBI Tokenisation Guidelines: card data must be tokenised — align tokenisation practices with DPDP data security requirements.
- IT (Intermediary Guidelines) Rules, 2021: marketplace platforms as intermediaries have grievance officer and due-diligence requirements — integrate with DPDP grievance redressal.
- TRAI Regulations on unsolicited commercial communications (UCC): telemarketing consent must be DPDP-compliant opt-in (not just DND exemption).
- Third Schedule, DPDP Rules, 2025: 3-year default retention for e-commerce entities with 2 crore+ users from last login or last transaction — compliance is mandatory.

PENALTY EXPOSURE	Up to ₹250 crore for security failures (payment data breaches). Up to ₹200 crore for children's data violations. Large platforms face SDF-level exposure of ₹150 crore for additional obligation breaches.

Compliance checklist

ACTION ITEM	PRIORITY	TARGET
Redesign checkout consent — decouple fulfillment from marketing/analytics	CRITICAL	Month 2–4
Implement age verification at account creation	CRITICAL	Month 3–5
Audit recommendation engine data inputs — specific consent for personalisation	CRITICAL	Month 3–5
Classify and re-paper all seller/logistics partner data processing agreements	CRITICAL	Month 3–6
Implement 3-year retention/deletion schedule (Third Schedule default)	HIGH	Month 4–6
Build My Data self-service rights portal	HIGH	Month 5–8
Review checkout UI for dark patterns in consent collection	HIGH	Month 2–3
Integrate Board breach notification into security incident response	HIGH	Month 3–4
Begin SDF readiness (DPO, DPIA, data audit)	HIGH	Month 6–9
Align with Consumer Protection E-Commerce Rules grievance requirements	MEDIUM	Month 4–5

SECTOR 05 OF 12

5. Telecommunications

Infrastructure-level data processor | Certain SDF designation | Deep integration with Aadhaar eKYC | TRAI regulatory overlap

Data landscape — what personal data is processed

- Subscriber name, address, KYC documents (Aadhaar, PAN, Passport)
- Call Detail Records (CDR): call logs, SMS logs, data usage records
- Device IMEI numbers, SIM registration data
- Location data: cell tower pings, GPS (for apps), roaming records
- Billing data: payment history, outstanding dues, plan details
- VoIP/OTT call logs if processed by the operator
- Customer support interaction records
- CCTV footage at service centres

Key DPDP risks & regulatory pressure points

- **Guaranteed SDF designation** — telecom operators processing CDRs of hundreds of millions of subscribers are near-certain SDF designees. DPO, DPIA, data audits, and algorithmic transparency will apply.
- **CDR and location data** — call and location records are among the most sensitive behavioral datasets — they reveal patterns of life, health conditions, religious practices, and associations. Breach or misuse risk is extreme.
- **Law enforcement data requests** — DPDP Act national security exemptions allow government data access — but operators must ensure requests are properly authorised and within defined scope.
- **TRAI overlap** — TRAI's Quality of Service regulations, tariff orders, and UCC frameworks all involve personal data. DPDP compliance must be layered on top of TRAI obligations.
- **eKYC via Aadhaar** — Aadhaar-based eKYC involves UIDAI and Aadhaar Act provisions — DPDP obligations exist alongside Aadhaar Act consent requirements.
- **Roaming and international subscriber data** — outbound roaming partners receive Indian subscriber data — cross-border transfer compliance required.

Implementation steps — sequenced action plan

- **CDR Data Governance** — Classify CDR and location data. Implement strict access controls, audit logging, and purpose limitation. CDRs for billing (legitimate use) vs. analytics (consent required) must be processed separately.
- **SDF Readiness Programme** — Begin DPO appointment, DPIA framework, and independent data auditor engagement immediately — telecom operators are the most likely early SDF designees.
- **Customer Consent Rebuild** — Subscriber consent at SIM activation currently covers only regulatory KYC. Separate: (a) KYC/connection (legal obligation), (b) marketing and loyalty programmes (fresh consent), (c) data analytics (fresh consent).
- **Aadhaar/eKYC Alignment** — eKYC data governed by Aadhaar Act and UIDAI guidelines — ensure DPDP notice and consent obligations are layered on top without conflicting. Retain minimal eKYC data post-verification.
- **Law Enforcement Interface** — Build a formal lawful-intercept governance framework — document each request against the DPDP national security exemption. Implement segregated systems for law enforcement access.
- **Breach Protocol** — CDR breach affecting millions triggers Board notification + mass individual notification. Build automated notification infrastructure.

Sector-specific special obligations

- Indian Telecommunications Act, 2023: subscriber data protection obligations — align with DPDP requirements.
- TRAI Customer Preference Regulations (DND): unsolicited commercial communication consent must meet DPDP standards.
- Aadhaar Act, 2016 and UIDAI Regulations: biometric data and Aadhaar numbers have their own regulatory overlay — Aadhaar Act consent requirements co-exist with DPDP.
- DoT Licensing Conditions: subscriber data retention requirements under licences — document as legal obligation basis for DPDP purposes.
- CERT-In Directions: cyber incident reporting within 6 hours — integrate with DPDP 72-hour Board notification.

PENALTY EXPOSURE	Maximum ₹250 crore for security failures. As SDFs, telecom operators face ₹150 crore for SDF obligation breaches. CDR breaches affecting millions of subscribers would attract the highest end of the penalty range.

Compliance checklist

ACTION ITEM	PRIORITY	TARGET
Begin SDF readiness programme — DPO appointment, DPIA, auditor engagement	CRITICAL	Immediate
CDR governance: access controls, audit logs, purpose separation (billing vs. analytics)	CRITICAL	Month 1–4
Redesign subscriber consent at SIM activation — decouple from marketing/analytics	CRITICAL	Month 3–5
Aadhaar/eKYC: post-verification deletion workflows; DPDP notice overlay	CRITICAL	Month 3–5
Law enforcement interface governance framework	HIGH	Month 4–6
Mass breach notification infrastructure	HIGH	Month 4–6
Roaming partner data-sharing agreements — DPDP clauses	HIGH	Month 4–6
Align with TRAI UCC regulations and new Telecom Act requirements	MEDIUM	Ongoing

SECTOR 06 OF 12

6. HR, Staffing & Payroll Services

Data Fiduciary for employer-clients AND for candidate/employee data | Employment legitimate use basis | Background verification data is highly sensitive

Data landscape — what personal data is processed

- Candidate: resume, educational certificates, previous employment details
- Background verification: criminal record checks, credit checks, address verification
- Biometric attendance: fingerprint/facial recognition for timekeeping
- Payroll data: bank accounts, salary slips, Form 16, TDS details, PF/ESI numbers
- Performance reviews, disciplinary records, promotion history
- Medical fitness certificates, pre-employment health checks
- Leaves and attendance records
- Identity documents: Aadhaar, PAN, passport, driving licence

Key DPDP risks & regulatory pressure points

- **Biometric data** — attendance systems using fingerprints or facial recognition process particularly sensitive data. Specific consent or documented legitimate use is required for biometric processing.
- **Background verification** — criminal record checks and credit checks involve sensitive data from third parties (police, bureaus). The scope of checks must be proportionate to the job role.
- **Employment legitimate use scope** — Section 7 allows processing without consent for employment purposes — but only for activities within the reasonable scope of an employment relationship. Sharing employee data with third-party analytics vendors or group companies exceeds this scope without consent.
- **Contractor and gig worker data** — staffing agencies process data for temporary workers placed at client sites. The staffing agency is typically the Data Fiduciary; the client is a Data Processor for certain purposes.
- **Departing employee data** — post-termination data retention — what can be kept, for how long, and for what purpose (e.g., tax compliance, reference checks) must be documented.

Implementation steps — sequenced action plan

- **Candidate Data Map** — Audit all data collected during recruitment (job portals, assessment platforms, interview recordings) — many third-party recruitment tools are sub-processors.
- **Biometric Consent** — Biometric attendance — obtain express, documented consent from employees. Provide an alternative attendance method for employees who do not consent.
- **Background Verification Governance** — Scope background checks proportionately. Obtain candidate consent for each category of check. Instruct verification agencies via DPDP-aligned processor agreements.
- **Payroll Processor Agreements** — Re-paper all payroll bureau and HRMS vendor agreements with DPDP processor clauses including deletion on termination.
- **Employee Notice** — Issue a comprehensive employee privacy notice covering: HR data collected, purposes, rights, and grievance contact.
- **Retention Schedule** — Post-employment retention: PF/ESI records (retain for statutory periods), Form 16 (7 years for income tax purposes), background check results (delete after hire/rejection), performance records (document retention basis).
- **Departure Workflow** — Build an employee exit data workflow: what is retained vs. deleted on departure, and notification to the departing employee.

Sector-specific special obligations

- Employees' Provident Fund and Miscellaneous Provisions Act, 1952: PF records retained for statutory periods — legitimate use basis under DPDP.
- Payment of Gratuity Act, 1972: gratuity eligibility records — legal obligation retention basis.
- Income Tax Act, 2025: Form 16, TDS records (7-year retention) — legal obligation basis.
- Shops and Establishments Acts (state-wise): employee records maintenance — document as legal obligation.

– POSH Act, 2013: ICC proceedings involving employees include sensitive personal data — process under legal obligation, maintain strict confidentiality.

PENALTY EXPOSURE	Biometric data breach — up to ₹250 crore. Payroll/financial data breach — up to ₹250 crore. Staffing agencies with millions of candidates in their databases face SDF designation risk.

Compliance checklist

ACTION ITEM	PRIORITY	TARGET
Obtain express consent for biometric attendance; provide alternative	CRITICAL	Month 1–3
Scope and document basis for each category of background check	CRITICAL	Month 2–3
Issue employee and candidate privacy notices	CRITICAL	Month 2–4
Re-paper payroll bureau, HRMS, and BGV vendor agreements	CRITICAL	Month 3–5
Build post-employment data retention/deletion schedule	HIGH	Month 3–5
Audit all third-party recruitment tools as sub-processors	HIGH	Month 3–4
Build employee rights workflow (access, correction, erasure requests)	HIGH	Month 4–6
POSH proceedings data — access control and retention governance	MEDIUM	Month 4–5

SECTOR 07 OF 12

7. Education — K-12, Higher Education & EdTech

Predominantly children's data — highest children's data compliance burden | EdTech platforms likely SDF candidates | Academic records are sensitive long-term personal data

Data landscape — what personal data is processed

- Student: name, date of birth, Aadhaar (for scholarship schemes), address
- Academic records: marks, grades, transcripts, certificates, result data
- Attendance records, disciplinary records, special education needs
- Parent/guardian contact details and financial information (fees, scholarships)
- Biometric data for exam-hall attendance and access control
- Online learning: video interaction, assignment submissions, quiz responses
- Proctoring data: webcam images, screen recordings, mouse/keyboard patterns
- Placement cell: student resumes, employer communications, offer letters
- Learning analytics: engagement scores, time-on-platform, completion rates

Key DPDP risks & regulatory pressure points

- **Children everywhere** — K-12 institutions and most EdTech platforms serve Data Principals who are predominantly under 18 — every student account requires verifiable parental consent before processing. This is a structural challenge at scale.
- **Online proctoring** — proctoring data (video, keyboard/mouse analytics) is highly sensitive behavioral biometric data. Specific consent is required. Storage duration must be limited and explicitly consented to.
- **Academic record permanence** — transcripts and certificates are retained for decades. The Act's deletion right conflicts with institutional record-keeping needs — document legal obligation basis carefully.
- **EdTech SDF risk** — platforms with 50 lakh+ child users are explicitly referenced in the Third Schedule (3-year retention from last login). Large EdTech players face near-certain SDF designation.
- **Learning analytics for AI** — EdTech companies using learning data to train personalisation algorithms need specific, separate consent — cannot rely on educational service consent for AI training.
- **Third-party integrations** — classroom tools (Google Classroom, Zoom, Microsoft Teams) are Data Processors — ensure processor agreements are DPDP-aligned.

Implementation steps — sequenced action plan

- **Age Gating & Parental Consent** — Implement age verification at student registration. For all students under 18, obtain verifiable parental/guardian consent before any data processing. Build parent consent portals.
- **Academic Record Retention Framework** — Document the legal obligation basis for long-term academic record retention (University Acts, UGC regulations, board regulations). Separate legally mandated records from operational data.
- **Proctoring Data Governance** — Limit proctoring data collection to the minimum necessary. Obtain specific, informed student/parent consent before each proctored exam. Define maximum retention (typically 30–90 days post-result declaration) and auto-delete.
- **EdTech Product Consent Flows** — Redesign onboarding consent: separate learning service consent from analytics, AI personalisation, and marketing consent. Build parent consent management interface.
- **Processor Contracts** — Re-paper all EdTech vendor, LMS, and classroom tool agreements. Ensure Google/Microsoft/Zoom educational agreements include DPDP processor clauses.
- **Learning Analytics Governance** — Audit all personalisation and recommendation algorithms for data inputs. Ensure specific parental consent for AI/analytics use of child learning data.
- **Placement Cell Data** — Student placement data (resumes, employer communications, offer details) is among the most sensitive — strict access controls, consent from students before sharing with employers, deletion on request.

Sector-specific special obligations

- UGC Regulations: universities must maintain student records as specified — documents as legal obligation basis for DPDP retention compliance.

– Right to Education Act, 2009: student data collected for RTE admission and scholarship schemes — State/government legitimate use basis applies.
– NEP 2020 and DIKSHA/SWAYAM platforms: government EdTech platforms process student data at scale — DPDP applies to State instrumentalities, subject to Second Schedule standards.
– CBSE/ICSE Board Examinations: result data processed by boards — legal obligation retention basis, but data sharing with third parties requires DPDP-aligned agreements.
– Third Schedule, DPDP Rules: 3-year default retention for online gaming entities with 50 lakh+ users — the same threshold is likely to be applied to large EdTech platforms with comparable user counts.

PENALTY EXPOSURE	Children's data violations — ₹200 crore. Security failures involving student databases — ₹250 crore. Large EdTech platforms will likely face SDF designation with additional SDF penalty exposure of ₹150 crore.

Compliance checklist

ACTION ITEM	PRIORITY	TARGET
Implement age verification + verifiable parental consent for all under-18 students	CRITICAL	Month 1–3
Redesign EdTech onboarding consent — separate service from analytics/AI	CRITICAL	Month 2–4
Proctoring data: consent before each exam, max 90-day retention, auto-delete	CRITICAL	Month 2–4
Document legal obligation basis for academic record long-term retention	CRITICAL	Month 2–3
Re-paper Google/Microsoft/Zoom/LMS processor agreements	HIGH	Month 3–5
Build parent consent management portal for minor students	HIGH	Month 4–7
Audit AI/personalisation algorithms for child data inputs	HIGH	Month 4–6
Placement cell data: student consent before employer sharing	HIGH	Month 3–4
Large EdTech platforms: begin SDF readiness (DPO, DPIA)	HIGH	Month 6–9
Student data breach response drill	MEDIUM	Month 6

SECTOR 08 OF 12

8. Real Estate, Property & Construction

Long data retention cycles | Buyer/tenant personal data at every transaction touchpoint | RERA compliance overlap

Data landscape — what personal data is processed

- Buyer/tenant: name, PAN, Aadhaar, contact details, income proof
- KYC for property purchase: Form 60, bank statements, salary slips
- Site visit logs, lead tracking data, broker interaction records
- Loan application data shared with NBFC/bank partners
- CCTV footage at construction sites, residential complexes, offices
- Resident association data: maintenance payments, parking records
- Tenant background verification: rental agreements, references
- PropTech: virtual tour interaction data, chatbot conversations

Key DPDP risks & regulatory pressure points

- **Long transaction cycles** — property transactions take months to close — lead data is held for extended periods. DPDP requires data to be deleted once the purpose (closing the sale/rental) is served or consent is withdrawn.
- **Broker and channel partner data sharing** — customer data shared with brokers, co-developers, and financial partners must be under DPDP processor or Fiduciary agreements.
- **CCTV in residential complexes** — CCTV footage of residents and visitors is personal data. Retention beyond operational necessity (typically 30–90 days) requires documented basis.
- **RERA compliance** — RERA requires allottee information to be maintained — legal obligation retention basis for certain data. RERA's disclosure obligations may conflict with data minimisation.
- **NRI and foreign buyers** — cross-border data sharing for international property transactions — FEMA + DPDP compliance intersection.

Implementation steps — sequenced action plan

- **Lead and CRM Data Governance** — Implement DPDP-compliant consent at lead capture (website, property portals, IVR). Define maximum lead retention period (12–18 months from last interaction); auto-delete stale leads.
- **KYC and Transaction Document Governance** — KYC documents (Aadhaar, PAN, income proof) collected for property transactions — document the legal obligation/contractual basis. Delete originals post-registration; retain copies for RERA/tax compliance.
- **Broker and Partner Agreements** — Re-paper all broker, channel partner, and NBFC referral agreements. Classify brokers as Data Processors or independent Fiduciaries based on their processing activities.
- **CCTV Policy** — Implement a published CCTV policy for residential complexes and project sites: purpose, retention (max 90 days), access controls, no sharing with third parties without legal basis.
- **Resident Data Governance** — Resident association/facility management data (maintenance payments, access logs) — issue a resident privacy notice; build a grievance mechanism.
- **PropTech Consent** — Virtual tour platforms and chatbots collect behavioral data — DPDP consent required for analytics and retargeting beyond session delivery.

Sector-specific special obligations

- RERA, 2016: allottee information maintenance and disclosure requirements — document as legal obligation basis for DPDP retention compliance.
- Registration Act, 1908 and Stamp Acts (state-wise): property registration documents include personal data — legal obligation retention basis.
- Prevention of Money Laundering Act (PMLA): real estate agents are reporting entities under PMLA amendments (2023) — KYC and transaction records (5 years) qualify as legal obligation basis.
- IT Act 2000 / SPDI Rules: currently operative for CCTV and digital data — transitions to DPDP Act.

PENALTY EXPOSURE	Financial data breach (income proofs, bank statements) — up to ₹250 crore. CCTV data breach — up to ₹250 crore. PropTech platforms with large user bases risk SDF designation.

Compliance checklist

ACTION ITEM	PRIORITY	TARGET
DPDP-compliant consent at lead capture (web, portals, IVR)	CRITICAL	Month 2–3
CRM stale lead auto-deletion (12–18 months from last interaction)	HIGH	Month 3–5
Re-paper broker, channel partner, and NBFC referral agreements	CRITICAL	Month 3–5
CCTV policy: retention max 90 days, published notice at sites	HIGH	Month 2–4
KYC document governance: secure storage, post-registration deletion/retention basis	CRITICAL	Month 2–4
Document RERA/PMLA legal obligation basis for long-retention data	HIGH	Month 2–3
Resident privacy notice for housing complexes/facility management	MEDIUM	Month 4–6
PropTech behavioral data consent — analytics and retargeting	HIGH	Month 3–5

SECTOR 09 OF 12

9. CA Firms, Legal, Consulting & Professional Services

Data Fiduciary for client and employee personal data | Intersection with CA/legal professional privilege | Engagement-specific data minimisation is critical

Data landscape — what personal data is processed

- Client identification: PAN, Aadhaar, GST, CIN, Director DINs
- Financial data: income, assets, liabilities, tax filings, bank statements
- Legal documents: agreements, notices, court orders, regulatory correspondence
- Business confidential: board minutes, internal policies, M&A data
- Audit working papers containing client employee personal data
- Valuation reports referencing individual shareholders
- HR/payroll data of client entities processed during audits
- Email correspondence with clients containing personal data
- Employee HR data of the firm itself

Key DPDP risks & regulatory pressure points

- **Engagement data vs. personal data** — client engagements often involve processing personal data of individuals (shareholders, employees, directors of client companies) who are not parties to the engagement — DPDP obligations extend to these Data Principals.
- **Long engagement data retention** — audit working papers are retained for 7–10 years (ICAI requirements). This is a legal obligation basis — but must be documented explicitly and access restricted.
- **Client personal data in emails** — unstructured personal data in email correspondence is digital personal data under the Act. Firms need email retention and deletion policies.
- **Cloud and collaboration tools** — firms using Google Workspace, Microsoft 365, or collaboration platforms — these are Data Processors. Ensure DPDP-aligned processor agreements.
- **Subcontracting** — work referred to other firms or outsourced to shared service centres involves personal data transfer — must be governed by sub-processor agreements.
- **Tax filing platforms** — firms using tax filing software (e.g., Taxmann, Winman, ClearTax) to process client returns — these platforms are Data Processors.

Implementation steps — sequenced action plan

- **Engagement Agreement Update** — Add a data processing clause to all engagement letters: what personal data will be processed, for what purpose, the firm's obligations as Data Fiduciary, and how clients can exercise rights.
- **Data Inventory by Engagement Type** — Map personal data processed for each service line: audit, tax, valuation, advisory. Identify Data Principals (not just the corporate client, but individuals whose data is processed).
- **Retention Schedule** — Audit working papers (7 years — ICAI), Form 16s and tax records (7 years — IT Act), valuation reports (3–5 years), legal documents (as applicable). Document each retention basis.
- **Cloud Tool Processor Agreements** — Re-paper Google Workspace, Microsoft 365, Dropbox, or ClearTax agreements with DPDP processor clauses.
- **Employee Privacy Notice** — Issue a firm-level employee privacy notice covering HR, payroll, and performance data.
- **Access Controls** — Client files should be accessible only to engagement team members. Implement role-based access in document management systems. Audit logs for all access.
- **Secure Communication** — Client personal data should not be transmitted over unencrypted channels. Enforce encrypted email (or secure client portals) for documents containing PAN, Aadhaar, financial data.
- **Breach Response** — A breach of client audit files or tax data is catastrophic reputationally. Build a breach response plan with ICAI notification protocols alongside DPDP Board notification.

Sector-specific special obligations

- ICAI Guidelines: audit working paper retention (7 years minimum) — legal obligation basis for DPDP purposes.
- Income Tax Act, 2025: tax records and Form 16 retention (7 years) — legal obligation basis.
- Companies Act, 2013: statutory registers and audit records — legal obligation retention basis.

– IBBI Registered Valuers Regulations: valuation reports and working files — document retention obligations as legal obligation basis.
– Prevention of Money Laundering Act: CA firms as Designated Non-Financial Businesses and Professions (DNFBPs) must maintain KYC records of clients for 5 years — legal obligation basis.
– Bar Council of India Rules (for legal firms): client confidentiality obligations run alongside DPDP — they are complementary, not conflicting.

PENALTY EXPOSURE	Breach of client financial data (income, tax, bank details) — up to ₹250 crore. Given the sensitivity and volume of data in professional-services databases, the penalty exposure is disproportionate to firm size — early compliance is essential.

Compliance checklist

ACTION ITEM	PRIORITY	TARGET
Add DPDP data processing clause to all engagement letters	CRITICAL	Month 1–2
Map personal data processed per service line (audit, tax, valuation)	CRITICAL	Month 1–3
Document retention basis for each data category (ICAI, IT Act, Companies Act, PMLA)	CRITICAL	Month 2–3
Re-paper cloud tool agreements (Google Workspace, M365, ClearTax, Winman)	CRITICAL	Month 3–4
Implement role-based access controls in document management systems	CRITICAL	Month 2–4
Enforce encrypted communication for client documents with personal data	HIGH	Month 2–4
Issue employee privacy notice for firm staff	HIGH	Month 2–3
Build breach response plan — DPDP Board + ICAI notification	HIGH	Month 3–5
Client rights workflow: access, correction, erasure requests within 90 days	MEDIUM	Month 4–6
Sub-processor agreements for referral firms and shared service centres	MEDIUM	Month 3–5

SECTOR 10 OF 12

10. Manufacturing, Supply Chain & Logistics

Employee and vendor personal data at scale | IoT/connected plant adds new data dimensions | Cross-border supply chains | Typically not SDF candidates — lighter compliance burden

Data landscape — what personal data is processed

- Employee: HR, payroll, biometric plant access, safety training records
- Contract workers: ID documents, contractor agency records
- Vendor/supplier personal data: proprietor/partner details, bank accounts
- Customer data (B2B typically non-personal; B2C more sensitive)
- IoT/SCADA data linked to individual operators (if identifiable)
- Delivery partner and logistics driver personal data
- Factory visitors: gate entry registers, CCTV footage
- Export/import documentation: individual shipper/consignee details

Key DPDP risks & regulatory pressure points

- **Biometric plant access** — fingerprint and iris scanners for plant entry and hazardous area access — requires specific employee consent or documented employment legitimate use.
- **Contract worker data** — high turnover means large volumes of onboarded and offboarded personal data — strict deletion workflows are needed.
- **Vendor due diligence** — KYC of vendor proprietors/partners (Aadhaar, PAN) collected for onboarding — must be deleted or anonymised after the vendor relationship ends.
- **Cross-border logistics** — export documentation involving personal data of overseas consignees and representatives — cross-border transfer tracking required.
- **IoT and plant analytics** — if machine performance data is linked to individual operators (shift supervisor, machine operator), it constitutes personal data.

Implementation steps — sequenced action plan

- **Employee and Contract Worker Governance** — Issue employee privacy notices. Implement biometric consent or document employment legitimate use. Build contractor onboarding/offboarding data workflows.
- **Vendor KYC Data Management** — Define retention for vendor KYC data (PAN, Aadhaar of proprietors): retain during the vendor relationship + 3 years post-termination for PMLA purposes, then delete.
- **CCTV Policy** — Factory CCTV: published notice at entry, 90-day retention maximum, access restricted to safety/security teams.
- **Supply Chain Platform Governance** — Procurement, logistics and supply-chain platforms processing personal data — classify as Data Fiduciary or Processor per usage. Execute DPDP agreements with enterprise clients using these platforms.
- **Cross-Border Documentation** — For export/import documents with individual personal data — ensure they are not retained beyond customs/DGFT retention requirements; document legal obligation basis.

Sector-specific special obligations

- Factories Act, 1948: employee records, accident registers — legal obligation retention basis.
- MSME Development Act: vendor payment data — legal obligation basis for retention.
- Customs Act, 1962 and DGFT Regulations: import/export documentation retention — legal obligation basis.
- PMLA: vendor KYC records (5 years) — legal obligation basis for extended retention.

PENALTY EXPOSURE	Employee biometric data breach — up to ₹250 crore. Most mid-size manufacturers are unlikely to face SDF designation — compliance burden is proportionately lighter.

Compliance checklist

ACTION ITEM	PRIORITY	TARGET
Biometric plant access: employee consent or documented employment legitimate use	CRITICAL	Month 1–3
Contractor onboarding/offboarding data workflow with auto-deletion	HIGH	Month 2–4
Vendor KYC retention schedule: active + 3 years post-termination	HIGH	Month 2–3
CCTV policy: 90-day retention, access controls, published notice	HIGH	Month 2–3
Supply chain platform processor/fiduciary role classification	HIGH	Month 2–4
Export documentation retention — Customs Act/DGFT legal obligation basis	MEDIUM	Month 3–4
Employee privacy notice (inclusive of IoT/operator-linked data)	HIGH	Month 2–4

SECTOR 11 OF 12

11. Media, Digital Platforms & Social Media

Highest SDF designation risk after telecom | Children's data at massive scale | Behavioral data monetisation model in direct tension with DPDP | Already regulated under IT Rules 2021

Data landscape — what personal data is processed

- Account data: name, email, phone, profile picture, location
- Behavioral data: content watched/read, search queries, time-on-platform, reactions
- Social graph: followers, following, group memberships, DM metadata
- Location data: check-ins, geo-tagged posts, IP-based inference
- Advertising profiles: interests, demographics, inferred characteristics
- Content: posts, comments, private messages, stories, reels
- Device data: OS, browser, IDFA/GAID, cookies
- Payment data (for subscriptions, in-app purchases)
- Age and identity (for age verification purposes)

Key DPDP risks & regulatory pressure points

- **Core business model tension** — digital advertising revenues are built on behavioral data profiling — the DPDP Act's granular consent requirements threaten the permissiveness of current 'accept all cookies' consent flows.
- **Children at scale** — social media platforms have large under-18 user bases. Age verification and parental consent requirements are technically and operationally challenging at 100M+ user scale.
- **Third Schedule** — social media with 2 crore+ users — 3-year retention default from last login explicitly prescribed. This is a signal of near-certain SDF designation.
- **IT Rules 2021 overlap** — significant social media intermediaries already have grievance officer, transparency reporting, and traceability obligations — these are a floor, not a ceiling, under DPDP.
- **Targeted advertising to children** — absolutely prohibited. Compliance requires reliable age determination — currently weak across most platforms.
- **AI content recommendation** — recommendation algorithms using personal data — SDF algorithmic transparency obligations will require disclosure of ranking and filtering logic.

Implementation steps — sequenced action plan

- **Consent Architecture Rebuild** — Replace cookie banners and bundled privacy policies with granular, purpose-specific consent: (a) core service, (b) personalisation, (c) advertising, (d) third-party sharing. Track consent at the user-feature level.
- **Age Verification at Scale** — Deploy robust age verification at account creation. For identified or suspected minor accounts: disable behavioral tracking, targeted advertising, and certain content categories.
- **Children's Advertising Prohibition** — Implement technical controls to prevent delivery of targeted advertising to under-18 accounts. This requires a combination of age signals and conservative default-off settings.
- **Advertising Data Governance** — Map the advertising data supply chain: user → platform → DSP/SSP → advertiser. Each handoff of personal data must be governed by DPDP-aligned agreements. Limit cross-context behavioral advertising without specific consent.
- **SDF Preparation** — Large platforms should begin DPO appointment, DPIA programme, and algorithmic transparency documentation now — they are the most likely early SDF designees.
- **Rights at Scale** — Build self-service portals for data access, download, correction, erasure, and consent withdrawal at platform scale. These must handle millions of requests.
- **Content Moderation Data** — Flagged content and moderation decisions linked to individual accounts — data retention and deletion obligations apply to these records too.

Sector-specific special obligations

- IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021: grievance officers, monthly transparency reports, traceability for significant social media intermediaries — DPDP adds to this, not replaces it.
- Third Schedule, DPDP Rules: 3-year retention for social media with 2 crore+ users from last login.

- IT Act Section 79 safe harbour: platforms lose safe harbour if they do not comply with government directions — DPDP Board directions carry the same weight.
- TRAI OTT regulation (evolving): communication platforms may face sector-specific data protection obligations beyond DPDP.
- Press and Registration of Periodicals Act: digital news publishers — editorial/journalistic exemptions under Section 17 may apply to news content processing.

PENALTY EXPOSURE	Largest penalty exposure of any sector: ₹250 crore for security failures; ₹200 crore for children's data violations; ₹150 crore for SDF failures. The Board is expected to make early high-profile enforcement examples in this sector.

Compliance checklist

ACTION ITEM	PRIORITY	TARGET
Rebuild consent architecture: granular, purpose-specific, opt-in	CRITICAL	Month 2–5
Age verification at account creation — implement robust age signals	CRITICAL	Month 3–6
Technical controls: no targeted advertising to under-18 accounts	CRITICAL	Month 3–6
Map advertising data supply chain — DPDP-aligned DSP/SSP/advertiser agreements	CRITICAL	Month 3–6
Begin SDF preparation: DPO, DPIA, algorithmic transparency documentation	CRITICAL	Month 4–8
Build self-service rights portal at platform scale	HIGH	Month 5–9
3-year retention schedule implementation (Third Schedule)	HIGH	Month 4–6
Align IT Rules 2021 grievance officer with DPDP grievance mechanism	HIGH	Month 2–3
Content moderation record governance	MEDIUM	Month 5–7
Breach notification at scale — automated Board and user notification	HIGH	Month 4–6

SECTOR 12 OF 12

12. Government, Public Sector Undertakings & State Instrumentalities

Both Fiduciary and exempt entity | Legitimate use basis covers most processing | National security exemptions are broad but must be formally notified

Data landscape — what personal data is processed

- Citizen service data: Aadhaar, PAN, ration card, voter ID
- Beneficiary data: subsidy disbursement records, welfare scheme beneficiaries
- Tax and revenue data: income, property, GST records
- Land and property records
- Healthcare data from government hospitals and PHCs
- Education data from government schools, universities
- Employee service records for government servants
- Law enforcement records (subject to specific exemptions)

Key DPDP risks & regulatory pressure points

- **Not fully exempt** — the DPDP Act applies to government bodies. The Second Schedule prescribes standards specifically for State processing under the Section 7(b) legitimate use basis — compliance is mandatory.
- **Aadhaar overlap** — much government citizen data is linked to Aadhaar. The Aadhaar Act and UIDAI regulations have their own data protection regime — DPDP layers on top.
- **Breach notification** — government databases are high-value breach targets. The Board notification and individual notification obligations apply to government entities as well.
- **PSU data sharing** — PSUs sharing citizen/beneficiary data with private sector partners (e.g., bank partnerships for subsidy disbursement) must execute DPDP-aligned processor agreements.
- **National security exemption** — broad but requires formal notification by the Central Government — cannot be self-invoked by agencies without proper authorisation.

Implementation steps — sequenced action plan

- **Citizen Service Data Mapping** — Map all digital citizen data across Ministries and departments. Classify processing activities by legitimate use category.
- **Second Schedule Compliance** — Government processing under Section 7(b) must meet the standards prescribed in the Second Schedule of DPDP Rules — document compliance with each standard.
- **PSU Processor Agreements** — Re-paper all private sector partner agreements where PSUs share citizen data.
- **Breach Response** — Government entities — including large PSUs — must comply with DPDP breach notification. Build incident response capabilities.
- **Employee Data Governance** — Government employee service records are personal data — issue privacy notices and build grievance mechanisms for government employees.

Sector-specific special obligations

- Aadhaar Act, 2016 and UIDAI Regulations: citizen Aadhaar data — dual compliance with Aadhaar Act and DPDP.
- RTI Act, 2005: information disclosed under RTI may include personal data — reconcile RTI disclosure obligations with DPDP privacy rights (Section 8(1)(j) RTI exemption for personal information is aligned with DPDP).
- Digital India initiatives (DigiLocker, UMANG, etc.): government platforms are Data Fiduciaries — DPDP applies.
- Second Schedule, DPDP Rules: specific standards for State and government processing.

PENALTY EXPOSURE	Government entities are subject to the full penalty framework. Breach of large citizen databases — up to ₹250 crore. PSUs with large data holdings are SDF designation candidates.

Compliance checklist

ACTION ITEM	PRIORITY	TARGET
Map all citizen and beneficiary digital data across Ministries/departments	CRITICAL	Month 2–4
Comply with Second Schedule standards for government processing	CRITICAL	Month 3–6
Re-paper private sector partner/PSU data-sharing agreements	HIGH	Month 4–6
Government employee privacy notice and grievance mechanism	HIGH	Month 4–6
Build breach response for government databases	CRITICAL	Month 3–5
Document national security exemption protocols — formal authorisation chain	HIGH	Month 3–5

APPENDIX

DPDP implementation master checklist (all industries)

The following universal checklist applies to every organisation, regardless of sector, as the foundation of DPDP compliance. Sector-specific items are in addition to these.

UNIVERSAL ACTION	OWNER	DEADLINE
Complete personal data inventory and flow mapping	DPO / Legal	Month 1–2
Establish Record of Processing Activities (RoPA)	DPO / Compliance	Month 2–3
Redesign all consents — opt-in, granular, withdrawable	Product / Legal	Month 3–5
Issue DPDP-compliant privacy notices in all relevant languages	Legal / Marketing	Month 3–4
Implement grievance redressal mechanism and publish contact	Ops / Legal	Month 3–4
Deploy security safeguards: encryption, access control, audit logs (at least 1 year)	IT / CISO	Month 2–6
Build breach detection and 72-hour Board notification capability	IT / CISO	Month 3–5
Execute DPDP-aligned contracts with all Data Processors	Legal / Procurement	Month 3–6
Define and implement data retention and deletion schedules	IT / Compliance	Month 3–6
Implement age verification and parental consent for under-18 users	Product / Legal	Month 3–6
Appoint DPO and engage independent auditor (SDFs)	Board / Leadership	Month 6–9
Conduct Data Protection Impact Assessments (SDFs)	DPO	Month 7–10
Train all staff on DPDP obligations and data handling	HR / Compliance	Month 4–6
Embed Privacy by Design in SDLC / product development	Engineering / Product	Month 4–8
Review and update programme as new Rules/SDF designations are notified	DPO / Legal	Ongoing

How Kredo helps

Kredo Analytics implements DPDP compliance end to end — readiness diagnostic, programme delivery, Significant Data Fiduciary readiness, and assurance or managed compliance — led by Chartered Accountants and lawyers on the Kredo team and engineered into your systems by the same people who build compliance software. Write to **info@kredo.in** or visit **kredo.in**.