Digital Personal Data Protection Act, 2023

DPDP Act: Key Concepts, Framework and Compliance

Nagpur Branch of WIRC of ICAI

CA Ajay Bhandari | FCA · DISA · CISA · ISO 27001 LA | Co Founder at Zorixx Consultech

18-04-2026

India's data reality — why a law was inevitable

936 M+
internet users in India (2024)

1.4 B
Aadhaar numbers issued

₹177 Cr
avg. data breach cost (IBM India 2024)

Notable Indian data incidents

2023	**CoWIN portal**	Health & ID data of millions exposed via Telegram bot
2023	**AIIMS Delhi**	6 TB patient data encrypted in ransomware attack
2022	**Aadhaar**	800M records reportedly listed for sale on dark web
2021	**Air India**	4.5M passenger records exposed via SITA system breach

CONTEXT · GLOBAL LANDSCAPE

Data Privacy Laws Around the World

137+ countries now have data protection legislation — here are the landmark frameworks.

EUROPE

GDPR

2018

Gold standard. Fines up to 4% of global turnover or €20M.

UNITED STATES

HIPAA

1996 · CCPA 2020

Sector-specific. No single federal law. State-level reform.

CHINA

PIPL

2021

GDPR-inspired. Strict cross-border transfer rules.

SINGAPORE

PDPA

2012 · Updated 2020

Pro-business. Balances innovation with privacy.

INDIA · THE NEW FRONTIER

DPDPA, 2023

Digital Personal Data Protection Act

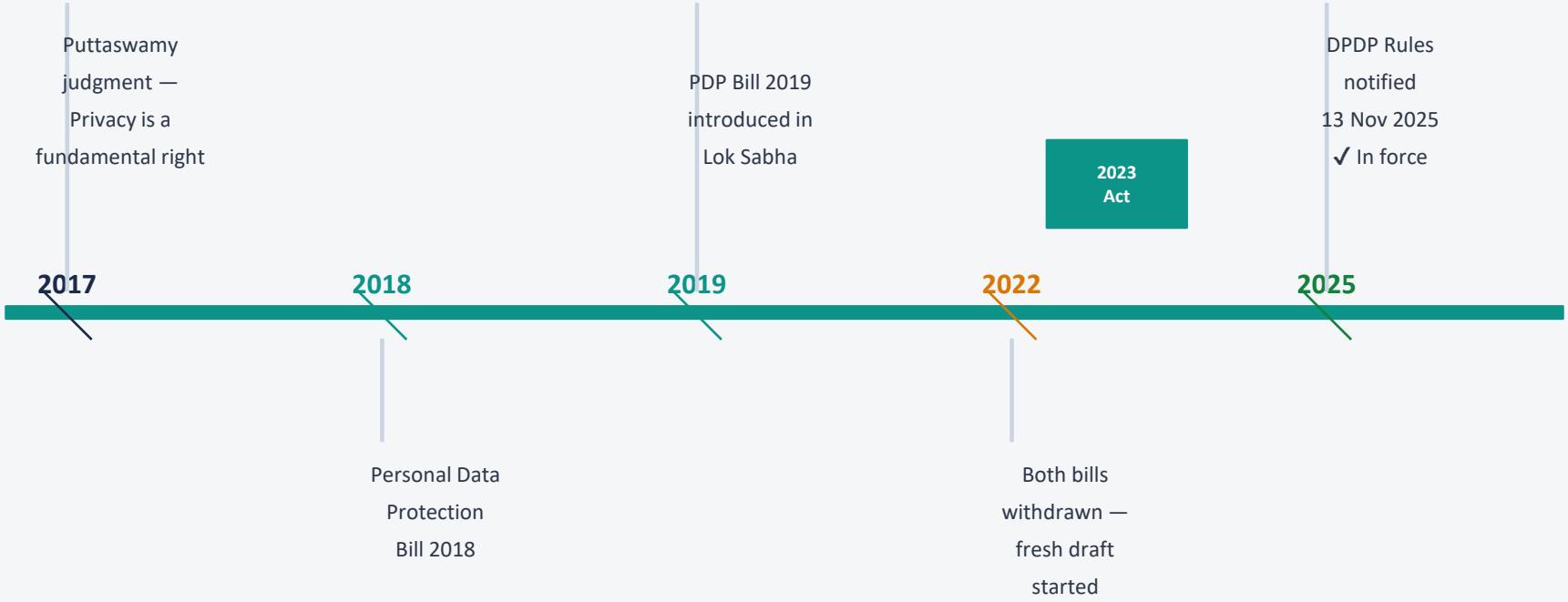
Enacted Aug 2023 · Rules notified Nov 2025 · Consent-centric · Compliance by May 2027

₹250 Crore Max Penalty

18 Months Compliance Window

1.4 Billion People Covered

The legislative journey



DPDP Rules 2025 notified 13 Nov 2025 · 23 Rules + 7 Schedules · Phased enforcement: Board (immediate) → Consent Managers (Nov 2026) → Full compliance (May 2027)

SESSION ROADMAP

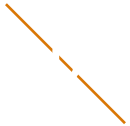
What will we cover today

Why this law?

Background & breaches

Act structure & scope

Definitions, roles



Consent & legitimate use

Two tracks + 3 exercises

Obligations & rights

DF duties · DP rights

Wrap-up & Q&A

Checklist · CA opps · QA

Separate sessions (not today): Penalties & enforcement · Business compliance requirements for clients · CA advisory framework

Data security vs data privacy vs data protection

Data Security

Technical safeguards that prevent unauthorized access, theft, or corruption of data.

- Firewalls & encryption
- Access controls & MFA
- Endpoint protection
- Intrusion detection

Data Privacy

Rights and choices individuals have over how their personal data is collected and used.

- User consent
- Purpose limitation
- Transparency
- Right to erasure

Data Protection

Legal framework creating accountability and governance — enforceable by regulator.

- Regulatory compliance
- Fiduciary obligations
- Penalties & enforcement
- Data Protection Board

DPDPA 2023 — Act at a glance (13 chapters)

Ch.I — **Preliminary**
Definitions · scope · who is covered

Ch.II — **Obligations of Data Fiduciary**
Notice · security · breach · grievance · deletion

Ch.III — **Rights of Data Principal**
Access · correction · erasure · grievance · nomination

Ch.IV — **Duties of Data Principal**
Accurate info · no false complaints

Ch.V — **Exemptions**
State · research · national security

Ch.VI — **Significant Data Fiduciary**
Enhanced obligations for large-scale DFs

Ch.VII–XIII — **DPB · Appeals · Penalties**
Data Protection Board · Appellate Tribunal · Fines

13 Chapters · 44 Sections · 23 Rules + 7 Schedules under DPDP Rules 2025 (notified 13 Nov 2025) · Phased enforcement: full compliance required by May 2027

What is 'data' and 'personal data'?

DPDPA applies only to digital personal data — information relating to an identifiable natural person.

Information

Any representation of information or opinion suitable for communication, interpretation, or automated processing.

Digital format required

Digital from origin (emails, forms, DBs) OR digitised from physical records. Both are covered.

Physical only = excluded

Paper files, handwritten ledgers — NOT covered. The moment you scan or photograph them, DPDPA applies.

Quick reference for CA practice

Client PAN card received by email / stored in cloud	✓ DPDPA applies
Scanned Aadhaar copy in Google Drive	✓ DPDPA applies
Tally / ERP records with client financial data	✓ DPDPA applies
Physical paper file in office cupboard (never scanned)	✗ Not covered
Aggregated industry fee benchmark (no individual identified)	✗ Not personal data

Types of personal data — direct and indirect identifiers

Direct identifiers

Name, email, mobile number

Identifies immediately — no combination needed

Government IDs

Aadhaar, PAN, Passport, Driving Licence

Official identifiers — unique to each person

Biometric data

Fingerprints, facial recognition, iris scans

Unique biological — highest sensitivity class

Indirect identifiers

IP address, device ID, location data

Identifies a person when combined with other data

Re-identification risk:
Anonymised or aggregated data becomes personal data if it can be combined with other information to re-identify an individual. Example: salary aggregate for a 3-person team may effectively reveal individual figures.

Audience quiz

Is this personal data under DPDPA?

Shoutout — YES or NO

1. A colleague's WhatsApp mobile number saved in your phone
2. Your CA firm's GST registration number
3. A scanned PAN card of a client stored in Google Drive
4. IP address of a visitor to your firm's website
5. An Excel of industry-average audit fees with no names or firm identifiers

Audience quiz

Is this personal data under DPDPA?

Raise your hand — YES or NO

1. A colleague's WhatsApp mobile number saved in your phone	YES	Direct identifier
2. Your CA firm's GST registration number	NO	Entity — not a person
3. A scanned PAN card of a client stored in Google Drive	YES	Digital + direct ID
4. IP address of a visitor to your firm's website	YES	Indirect identifier
5. An Excel of industry-average audit fees with no names or firm identifiers	NO	Anonymised aggregate

What does DPDPA cover — and what is exempt?

Fully covered

Digital personal data

- Emails, cloud files, digital forms
- ERP/Tally with client data
- Scanned docs, photographs
- WhatsApp with client data

Covered after digitisation

Physical → digital

- Paper form scanned to PDF
- Handwritten doc photographed
- Register entered into Tally
- Covered from moment of scan

Not covered

Purely physical records

- Paper files in office cupboard
- Handwritten ledgers never digitised
- Verbal communications
- Physical registers never scanned

Key exemptions — Section 17

- Personal / domestic use — individual processing own family data
- Research, archiving, statistical purposes — with adequate safeguards
- Startups & small entities — threshold to be notified by Rules

Where Does DPDP Apply?

- **Digital personal data** processing
- Processing **within or outside India**
- **Foreign companies** targeting Indian individuals (goods/services)
- **No turnover threshold** for applicability
- **No MSME exemption** currently

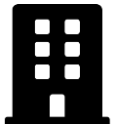
Key roles under DPDPA

Data Principal

Whose data it is

Example:

Your client · Your employee · You



Data Fiduciary

Decides purpose & means

Example:

CA firm · Bank · Company

Data Processor

Processes on DF's behalf

Example:

Cloud provider · Payroll vendor

Significant Data Fiduciary (SDF)

Enhanced obligations for DFs processing large volumes or sensitive data. Criteria notified via Rules (thresholds pending).

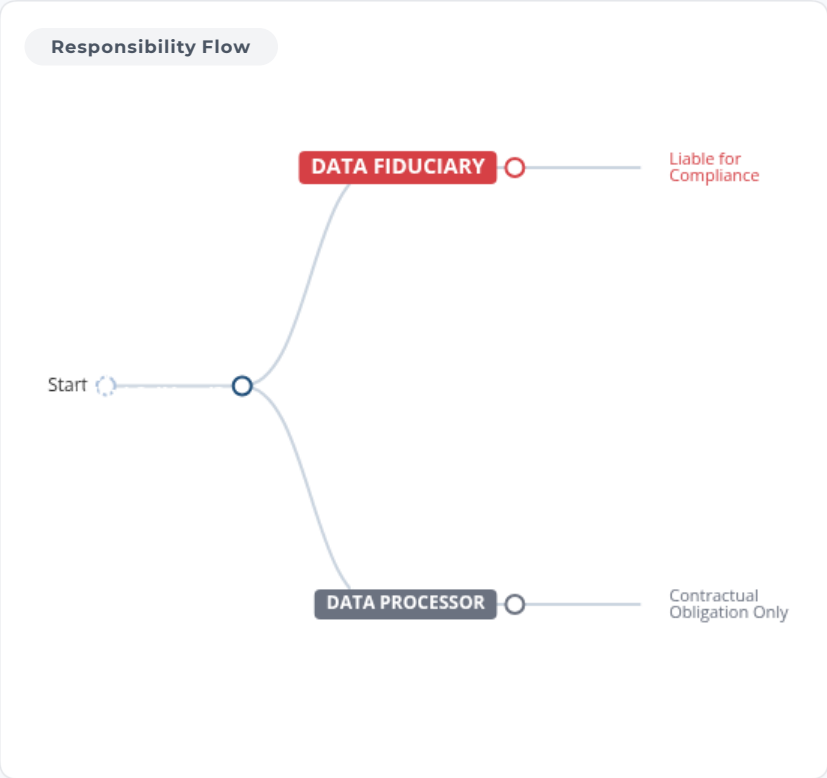
Consent Manager (CM)

Registered with DPB. Min net worth ₹2 crore. Must be a company incorporated in India. Manages consent on behalf of DPs.

⚡ **Every CA firm — regardless of size — is a Data Fiduciary. Compliance is mandatory, not optional.**

Where Does Responsibility Lie?

Understanding the core accountability principle under the DPDPA, 2023.



The "Means and Purpose" Test

Responsibility for compliance always rests with the entity that determines the key aspects of processing:

Why data is collected
Determining the purpose (e.g., payroll, marketing).

How it is used
Deciding the means of processing and analysis.

How it is protected
Setting security standards and safeguards.

> **"The Data Fiduciary carries primary accountability."**
>
> **Even if processing is outsourced, the buck stops with the Fiduciary.**

Only two lawful bases for processing personal data

Track A · Section 6

Consent

- Explicit, informed agreement from Data Principal
- Prior notice mandatory (Section 5 + Rule 3)
- Can be withdrawn at any time
- Cannot be bundled with service terms
- Data Principal rights fully attach

OR

Track B · Section 7

Legitimate Use

- Closed list of 9 specific grounds in the Act
- No consent or notice needed (mostly)
- Data protection principles still fully apply
- Over-collection still prohibited
- Purpose limitation still applies

Any processing outside these two tracks is unlawful. Penalty up to ₹250 crore per incident. Full penalty session: separate date.

Consent — 5 requirements + notice obligation

Free

No coercion. Cannot be made precondition for service. Power imbalance negates consent.

Specific

Purpose-bound. Separate consent for each distinct purpose — tax, audit, advisory, marketing.

Informed

Clear notice in simple language: data collected, purpose, retention period, rights.

Unambiguous

Affirmative action required. No pre-ticked boxes. Silence is NOT consent.

Revocable

Withdrawal as easy as giving consent. One-click mechanism. No barriers or justification needed.

Section 5 + Rule 3 — what every notice must contain:

(i) Personal data to be collected and the purpose for which it is proposed to be processed

(ii) How the Data Principal may exercise rights under S.6(4) and Section 13

(iii) How the Data Principal may make a complaint to the Data Protection Board

Legitimate uses — Section 7 (closed list of 9 grounds)

✓ DPDP Rules 2025 notified

S.7(i) categories still pending

Ground	Section	CA / common example	Notice?
Voluntary provision by DP (no objection stated)	7(a)	Client voluntarily provides business contact for follow-up	No
State / instrumentalities — subsidy, benefit, service	7(b)	UIDAI, PDS, passport office processing citizen data	Intimation
State function / sovereignty / security	7(c)	State performing function under any law, or national security	No
Legal obligation to disclose to State	7(d)	Banks disclosing suspicious transactions to FIU under PMLA	No
Court / judgment / decree / order compliance	7(e)	Sharing client data pursuant to court order or SFIO direction	No
Medical emergency / epidemic / disaster	7(f/g)	Hospital processing next-of-kin; state contact tracing	No
For safety during a disaster	7(h)	Identifying persons who might be leaving in flood affected area	No
Employer- Employee relationship	7(i)	An employer monitoring employee system access logs to prevent data leaks or fraud without taking consent.	No

EXERCISE 1 · 5 minutes

Spot the violations — fill this form

What YOU do — 3 steps

1

Open link

Open the Google Form on your phone. You'll see a client onboarding form from 'Zorixx Advisory'.

2

Read and Interpret

Fill your name, email, mobile. Tick the checkbox. Hit Submit. Takes 60 seconds.

3

Ask yourself one thing

Before I submitted — was I told what this firm will DO with my data? How long will they keep it? How do I get it deleted? Write your answer on paper.

https://dataprivacy-notice.netlify.app/

Exercise 1 debrief — Violations in the notice

Discussion upon the deficiencies

Password- zorixx2026

Core obligations of every Data Fiduciary

Privacy Notice S.5 / Rule 3

Transparent, standalone notice at point of collection — data, purpose, retention, Data Principal rights.

Security Safeguards S.8(4)/Rule 6

Encryption, access controls, monitoring logs (min 1 year), backup, vendor DPAs, anomaly detection.

Breach Reporting S.8(6)/Rule 7

Notify affected DPs without delay. Report to DPB: initial description immediately, detailed within 72 hours.

Grievance Redressal S.13/Rule 14

Accessible grievance contact. Respond within 7 days (Rule 14). Escalation: Data Protection Board.

Data Deletion S.8(7)/Rule

Secure deletion once purpose served. Notify DP at least 48 hours before erasure to allow last-chance exercise of rights.

Core Compliance Pillars

Five foundational principles that every Data Fiduciary must adhere to.

New opportunities for Chartered Accountants

DPDPA creates an advisory and assurance market — CAs are well-positioned to serve it.

DPDPA Gap Assessment

Baseline review of consent journeys, data mapping, security controls, retention. Actionable roadmap.

Privacy Audits

Periodic audit of processing activities, vendor compliance, breach readiness — structured like an IS audit.

Virtual DPO / Retainer

Fractional Data Protection Officer for SMEs. Governance oversight without full-time resource cost.

DPIA for high-risk work

Data Protection Impact Assessment for new digital products, large-scale processing, or sensitive data projects.

Full advisory framework, service line structuring, and client engagement model: covered in a separate dedicated session.

8 Advisory Opportunities

Each step is a billable CA engagement

Services

Engagement: 14–16 weeks | One-time + recurring fees | Client deadline: May 2027 | 8 opportunities

Data Discovery & Mapping

2-4 weeks

Cross-functional

30%

Data Inventory

Gap Assessment

1-2 weeks

Compliance/Legal

50%

Gap Report

Risk Analysis

Policy Drafting

4-8 weeks

Legal + IT

55%

Privacy Policy

Notice

Security Controls

4-12 weeks

IT/Security

65%

Security Matrix

Access Controls

Governance & vDPO

2-6 weeks

HR/Compliance

75%

Roles

Training

Contract Review

4-12 weeks

Legal/Procurement

85%

DPAs

Contracts

Privacy Audit

2-4 weeks

Compliance/IT

90%

Test Results

SOPs

Managed Compliance

Ongoing

Governance/Risk

100%

KPI Dashboard

Reviews

Opportunity 1: DPDPA Gap Assessment

Your entry-point engagement for every client

Duration: 1-2 weeks

What You Assess

Consent & Notice

Free, specific consent before processing?

Priority

Retention

Data deleted after a retention period?

Priority

Vendor Contracts

DPA & breach clauses in vendor contracts?

Priority

Security Controls

Access controls, encryption, audit logs?

Priority

Cross-border Flows

Vendors processing data outside India?

Priority

Children's Data

Under-18 users? Parental consent verifiable?

Priority

What You Deliver

Prioritized Gap Report (Red/Amber/Green)

- **Red Gaps:** Consent, breach notification, children's data (must address urgently)
- **Amber Gaps:** Retention, vendor contracts (resolve before May 2027)
- **Green Items:** Require monitoring only

Quick Wins for Clients

Immediate actions: Remove pre-ticked boxes, publish Grievance Officer, create retention schedule.

Evidence to Collect

Screenshots: Consent flows, policies, foreign-hosted systems

Opportunity 2: Data Discovery & Mapping

Find, classify & map clients' personal data

2–4 week engagement

What to Map

Data Categories
Employee, Customer, Vendor, etc.

Sources
Forms, website, verbally

Systems
CRM, HR system, Excel files

Data Owners
Department responsible

Legal Basis
Consent or Legitimate Use

Data Sharing
Internal/external sharing

Retention Period
30 days, 7 years, etc.

Third Parties
Vendors, processors

What You Deliver

Data Inventory Register

- ✓ Complete data processing activities record
- ✓ Dept questionnaires completed
- ✓ IT asset list with locations

Where Clients Struggle

Shadow IT: Spreadsheets, WhatsApp groups, personal emails

Mobile Apps: Unknown data collection permissions

Opportunity 3: Policy & Notice Drafting

Draft the document set every Data Fiduciary must publish

Policies

1. Privacy Policy (Public-Facing)

Key Requirements: Data categories, purpose, sharing, rights, Grievance Officer

Must Include: How to withdraw consent, data principal rights

Section 8 of DPDP Act

2. Consent Notice (Point of Collection)

Key Requirements: What data, why, how long, withdrawal mechanism

Affirmative Action: No pre-checked boxes, active consent required

Section 6 of DPDP Act

3. Data Retention Policy

Key Requirements: Retention periods for each data category

Statutory Mapping: IT Act (7 yrs), Companies Act (8 yrs), PMLA (5 yrs), GST (8 yrs)

Multiple Acts

4. Grievance Standard Operating Procedure

Key Requirements: Intake channel, ID verification, routing, timelines

Timeline: 30 days for resolution, escalation path to DPB

Section 13 of DPDP Act

5. Incident Response Plan

Key Requirements: Roles, 72-hr DPB notice, CERT-In alignment

Breach Notification: Who declares, who notifies, customer comms

Section 8(6) of DPDP Act

Opportunity 4: Security Controls Advisory

Advise clients on the safeguards Section 8(5) demands

Security

Section 8(5): "The Data Fiduciary shall implement appropriate technical and organisational measures to ensure effective observance of the provisions of this Act."

Access Control (RBAC)

- **Role-Based Access Control:** Implement RBAC to ensure employees access only data necessary for their function
- **Least Privilege:** Grant minimum permissions required for job function
- **Access Revocation:** Remove access within 24 hours of employee resignation

Encryption (At Rest & Transit)

- **Data at Rest:** Encrypt customer databases, HR systems, financial records
- **Data in Transit:** Use HTTPS/TLS for all web application traffic
- **Secure File Transfer:** Use encrypted portals instead of email for sensitive data

Audit Logs

- **Access Logging:** Record who accessed what data and when
- **Modification Tracking:** Log all changes to personal data
- **Retention Period:** Keep logs for appropriate duration for audit purposes

Vendor Security Review

- **ISO 27001:** Verify vendor certifications and security standards
- **Data Residency:** Confirm where data is physically stored
- **Breach SLA:** Ensure vendor notifies within agreed timeframe

Opportunity 5: Governance, vDPO & Training

Fractional DPO, role design & staff training

Duration: 2-6 weeks

Roles You Help Appoint

Grievance Officer

Required

Mandatory appointment under Section 13. Must be a named individual, not a generic email. Contact details must be published in Privacy Policy, website, and app.

Data Protection Officer (DPO)

SDF Only

For Significant Data Fiduciaries only. Based in India, reports to Board of Directors. Independent oversight function bridging governance and operations.

Opportunity: bundle with internal / IS audit work

Training You Deliver

Required Training Topics

- What is personal data
- Handling rights requests
- Breach reporting
- Acceptable use policies

Evidence Documentation

- Appointment letters
- Training records
- Org chart
- Policy acknowledgments

Culture Requirements

- No WhatsApp for KYC
- Clean desk policy
- Data labeling

Opportunity 6: Contract & DPA Review

Review DPAs, HR docs & engagement letters

Contracts

A) Vendor Data Processing Agreement (DPA)

Purpose-limited processing with security standards

- **Purpose Limited** — Processing only for defined purposes
- **Security Standards** — Must maintain adequate security
- **Breach Notice** — Notify promptly if breach occurs
- **Data Deletion** — Delete/return data on termination
- **Sub-processing** — No sub-processing without consent

B) Employment & HR Documents

Lawful basis = legitimate use, not consent

- **Lawful Basis** — Document as legitimate use
- **Retention Policy** — Specify retention periods
- **Access Revocation** — Revoke access on termination
- **CCTV Policy** — Office monitoring retention
- **Exit Procedures** — Data deletion at exit

C) CA Engagement Letters

Define Fiduciary vs Processor roles

- **Fiduciary Role** — Decide purpose & means
- **Processor Role** — Process on client instructions
- **Breach Notification** — Notify within agreed timeframe
- **Data Deletion** — Delete client data on exit
- **Cross-border** — Disclose data transfers

Engagement: review contracts, add DPA clauses, update engagement letters

High Priority | Immediate

Opportunity 7: Privacy Audit & Testing

Readiness drills run like an IS audit

Duration: 2-4 weeks

Drills You Run

Test 1: Data Access Request

30 days SLA

Client requests all personal data held

Track: find handler, verify ID, extract data

Test 2: Erasure Request

Subject to legal holds

Client asks to erase all their data

Track: delete across CRM, backups, vendors

Test 3: Breach Response Drill

72 hours

IT reports a weekend server breach

Track: declare incident, notify DPB & client

Metrics You Report

Time-to-assign	4 hrs
Time-to-collect	2 days
System coverage	92%
Notification readiness	78%

Deliverable: findings report + updated SOPs

Opportunity 8: Managed Compliance / Retainer

Recurring retainer to keep clients compliant

∞Ongoing

What You Monitor

SDF Notifications — Pending
Track Significant Data Fiduciary designations

Cross-Border Whitelist — Active
Monitor permitted countries for data transfers

DPB Guidance — Pending
Track enforcement guidance and updates

Annual Cycle You Run

- Policy Review
- Data Register
- Gap Assessment
- Vendor Re-checks

Reporting You Provide

Key Performance Metrics

Rights Request SLA **94%**	Breach MTTR **2.5 hrs**
Vendor DPA Coverage **87%**	Training Completion **98%**

Governance Reporting

- Quarterly Board Reports
- Audit Plan for SDFs
- Compliance Reviews

Two Core Principles

The bedrock of data protection architecture: defining boundaries and limits.

Purpose Limitation

Personal data collected for one specific purpose **must not be used** for another unrelated purpose.

Key Requirement:

- ✓ Strict adherence to Notice
- ✓ No "Mission Creep" or secondary use

Data Minimization

A Data Fiduciary shall collect **only what is necessary** for the specified purpose and nothing more.

Key Requirement:

- ✓ Processing must be "Necessary"
- ✓ Avoid "Nice-to-have" data points

Practical Challenge: Excessive Collection

"Do you really need Aadhaar, PAN, passport, *and* voter ID just for identity verification?" Collecting all four when one suffices violates the principle of Data Minimisation.

Children’s Data & Data of Persons with Disabilities

Verifiable guardian consent & safeguards for children (under 18) and persons with disabilities under DPDPA, 2023.

Children (Below 18)

Verifiable parental consent is mandatory before processing.

Strictly Prohibited:

- ✓ Tracking / behavioural monitoring
- ✓ Targeted advertising & processing likely to cause harm

Persons with Disabilities

Consent from **lawful guardian** is required where a person with disability has a legally appointed guardian.

Processing Must Be:

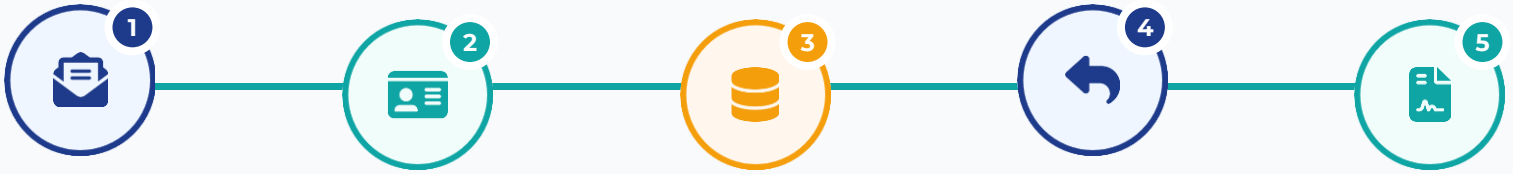
- ✓ Lawful, fair & transparent
- ✓ Consent + Legitimate Use (Sec 7)

Key Compliance Controls & Regulatory Note

Age/capacity verification, guardian consent workflows (OTP, KYC, digital), purpose limitation, accessible notice, secure retention/deletion & audit trails. **No tracking/monitoring unless specifically exempted by Government notification;** non-compliance carries significant penalties and reputational risk.

Storage Limitation - Data Governance Lifecycle

Handling a Data Access Request



Request Received

Log request from Data Principal via designated channel.

Identity Verification

Authenticate requester to prevent unauthorized access.

Data Extraction

Retrieve personal data and processing summary.

Response to Individual

Share information in clear, concise manner within timeline.

Record in Log

Document the request closure for audit trails.

Prescribed Timeline Compliance

The Data Fiduciary must respond within the period prescribed by the rules (likely to be 30 days). Failure to adhere to timelines can be treated as a deemed refusal, escalating to a grievance.

Initiation Processing Action

Rights of the Data Principal — Chapter III

S.11	**Right to access information** Know what personal data the DF holds, what it is used for, and to whom it has been disclosed or transferred.
S.12	**Right to correction & erasure** Correct inaccurate or outdated data. Request erasure when the purpose for which data was collected has been served.
S.13	**Right to grievance redressal** Raise a complaint with the DF's grievance officer. Unresolved → escalate to Data Protection Board (Rule 14: 7-day response).
S.14	**Right to nominate** Nominate any person to exercise Data Principal rights in the event of death or incapacity.
S.6(4)	**Right to withdraw consent** Withdraw consent at any time. DF cannot make withdrawal onerous. Effects on prior processing are not retrospective.

Breach reporting (per DPDP Rules 2025) + penalty snapshot

Breach response — Rule 7

1. Detect / suspect breach
2. Contain immediately
3. Notify DPs without delay
4. Report to DPB: initial now + details in 72 hrs
5. Document & implement controls

Breach notification to DPs: concise & clear — describe breach · likely consequences · mitigation steps · safety measures for DP · DF contact info.

Penalty snapshot (full penalty session: separate date)

Breach / violation	Penalty up to
Failure to implement security safeguards (resulting in breach)	₹250 crore
Breach of obligations for children's data	₹200 crore
Failure to notify DPB / affected DPs of breach	₹200 crore
Violation of consent / notice obligations	₹50 crore
Violation of other provisions of the Act	₹50 crore

DPDP Rules 2025 — what is in force and when

Phase 1

13 Nov 2025
Immediate

- DPB constituted (4 members)
- Board powers operative
- Penalty schedule operative
- Consent Manager registration process defined

Phase 2

13 Nov 2026
+12 months

- Consent Manager operations begin
- CM registration with DPB
- Penalty framework for CMs enforced
- Organisations assess CM integration needs

Phase 3

13 May 2027
+18 months (full)

- All consent obligations (S.6, Rule 3) enforced
- All DF obligations (S.8/Rule 6/7) enforced
- SDF obligations operative
- IT Act S.43A/SPDI Rules repealed

Thank You

Questions & open discussion

CA Ajay Bhandari | FCA · DISA · CISA · ISO 27001 LA

P C Bhandari & Co.

Mobile: 9158001588

Email: ajay.bhandari@zorixx.com

LinkedIn: linkedin.com/in/ajay-bhandari-jpm189189

ZORIXX