DPO ASSOCIATION OF INDIA

Welcomes you all

Sponsored by HKIT Security Solutions

Digital Personal Data Protection Act 2023

& Rules 2025 — Comprehensive Webinar

Covering: Enforcement Timelines · Governance · Consent · Data Rights · Breach · DPIA · and more

Governance	Privacy Notice	Consent	Data Inventory	Data Rights	Children's Data	Cross-Border
Fiduciary Duties	Processor Mgmt	DPIA	Retention	Breach Mgmt	Grievance	

Enforcement Timelines

When does each obligation take effect?

DPDP Act § Section	Rules	Obligation	Timeline
S.6(8) S.6(9)	Rule 4	Registration and obligations of Consent Manager	One year from publication date
S.3	—	Applicability of the Act	18 months from notification
S.5 S.6(10)	Rule 3	Notice given by Data Fiduciary to Data Principal	18 months from notification
S.9	R.10,12	Processing of personal data related to children	18 months from notification
S.10	Rule 13	Obligations of Significant Data Fiduciary (SDF)	18 months from notification
S.11–14	Rule 14	Rights of Data Principals	18 months from notification
S.16	Rule 15	Transfers of personal data outside India	18 months from notification

Key Timelines in the DPDP Rules

Critical deadlines every organization must operationalize

Rule 7(1)–7(2)

Breach Notification

Immediate + 72 Hours

First intimation to DPB: without delay
Detailed breach report to DPB: within 72 hours

Rule 8(2) + Sch.3

Data Retention & Erasure

3 Years + 48 hrs notice

E-commerce / social / gaming platforms retain data 3 years. Notify user 48 hrs before deletion.

Rule 13(1)

DPIA & Audit (SDF)

Every 12 Months

Significant Data Fiduciaries must conduct DPIA and independent audit yearly from Nov 2025 or SDF notification date.

Sch. 1 Part B-4(c)

Consent Records (Consent Manager)

7 Years

Consent managers must maintain records of consents, notices, and data-sharing activities for 7 years.

Rule 14(3)

Grievance Response

90 Days

Data Fiduciaries must respond to Data Principal grievances within 90 days of receipt.

DPDPA Framework

13 Integrated Components for End-to-End Compliance

01 **Governance & Accountability**

02 **Privacy Notice**

03 **Consent Management**

04 **Data Inventory & Mapping**

05 **Data Principal Rights**

06 **Children's Data Compliance**

07 **Cross-Border Transfers**

08 **Fiduciary Obligations**

09 **Processor Mgmt & Contracts**

10 **Risk Mgmt & DPIA**

11 **Data Retention & Deletion**

12 **Breach Management**

13 **Grievance Redressal**

Governance, Roles & Accountability

Who is responsible for what under DPDP?

Data Fiduciary (DF)

- Determines WHY & HOW data is processed
- Bears primary legal accountability
- Must implement privacy governance framework
- Responsible even if processor causes breach

Data Principal (DP)

- The individual whose data is processed
- Has rights: access, correction, erasure, nomination
- Can withdraw consent at any time
- Can file grievances with DPB

Data Processor

- External entity processing on DF's behalf
- Acts ONLY on DF instructions
- Bound by contractual obligations
- Cannot sub-delegate without DF approval

⭐ Special Role: Data Protection Officer (DPO)

- Mandatory for Significant Data Fiduciaries (SDFs) notified by Central Government
- Must be Indian resident • Reports directly to Board of Directors
- Acts as point of contact for grievance escalation to DPB
- Monitors compliance, audits, and DPIAs

Privacy Notice

What must be communicated to users before collecting their data?

📋 Notice Must Include

1. Purpose of data processing
2. Categories of personal data collected
3. Data Principal's rights under DPDP
4. How to withdraw consent
5. Grievance redressal contact details
6. Data retention practices & timelines

Format Requirements (Rule 3)

- ✓ Simple & easy to understand — no legal jargon
- ✓ Accessible in English or 8th Schedule languages
- ✓ With links to exercise rights & withdraw consent

When?

- Before or at the time of seeking consent
- Separate, standalone notice — not bundled with T&Cs
- Must be re-issued if purpose changes
- Prior notice required for processing children's data

Consent Management

Valid consent is the cornerstone of DPDP compliance

FREE	SPECIFIC	INFORMED	UNCONDITIONAL	UNAMBIGUOUS
No coercion, pressure, or conditional bundling with unrelated benefits	Linked to a single, clearly defined purpose — not blanket consent	User understands what they are consenting to through clear notice	Cannot be tied to unrelated services or mandatory extras	Requires explicit, affirmative action — pre-ticked boxes are invalid

Additional Requirements

- Obtained before processing personal data
- Linked to clearly stated purpose
- Recorded, auditable & traceable

Withdrawal of Consent

- Must be as easy as giving consent
- Cannot result in service denial (except where necessary)
- No discrimination against users who withdraw

Data Inventory & Mapping

Know your data — before regulators ask

Organizations Must Know:

- What personal data they collect
- Where they collect it from
- How data flows inside their environment
- Who they share it with (3rd parties)
- Where it is stored (location)
- How long it is retained (retention period)

Best Practices

- → Maintain structured data inventories
- → Use RoPA (Record of Processing Activities)
- → Tag personal & sensitive data elements
- → Link to risk ownership & processing purposes
- → Conduct regular data flow assessments
- → Keep inventory updated with each new system/vendor

✓ DPIA

Risk assessment relies on accurate data maps

✓ Retention

Know what to delete and when

✓ Access Mgmt

Limit access based on data sensitivity

✓ Breach Response

Identify scope of breach instantly

Data Principal Rights

Empowering individuals with control over their personal data

01

Right to Access

Know what personal data is collected, why it is collected, and with whom it is shared.

02

Right to Correction

Request correction or updating of inaccurate, incomplete, or outdated personal data.

03

Right to Erasure

Request deletion when purpose is fulfilled, consent withdrawn, or data no longer needed.

04

Right to Nomination

Appoint a nominee to exercise data rights on behalf of the Data Principal in case of death or incapacity.

Data Fiduciaries MUST provide:

- Simple & transparent mechanisms to exercise rights
- Time-bound responses (max 90 days under DPDP Rules)
- No coercive charges for processing rights requests
- Clear escalation path to DPB if unresolved

Children's Data Compliance

Special safeguards for users under 18 years of age

< 18

Definition of
'Child' under DPDP

Parental Consent Required

- Verifiable consent from parent / lawful guardian must be obtained BEFORE processing children's data. Verification via DigiLocker / OTP / KYC methods.

Prohibited Processing

- No tracking, monitoring, profiling, or behavioural advertising targeting children. No content or services harmful to children's well-being.

Age Verification

- Data Fiduciaries must implement verified age-gating mechanisms. Rule 10 specifies approved verification methods including DigiLocker integration.

Key Obligations

✓ Age verification system mandatory
✓ Parental consent workflows must be built into onboarding
✓ Child-friendly UI/UX with clear language
✓ No profiling or targeted advertising for children
✓ Exemptions exist for healthcare providers & educational institutions (limited scope)

Cross-Border Data Transfer Policy

India's approach: allow-by-default, restrict-by-notification

IN INDIA — DPDP

- Allow-by-default approach — transfers permitted unless government restricts
- Central Government issues 'negative list' of restricted countries
- Standard contractual clauses + adequate safeguards required
- No transfer if it compromises national security, sovereignty, or DP safety

EU EU — GDPR (Contrast)

- ↔ Restrict-by-default approach — transfers only to adequacy-approved countries
- ↔ Requires formal adequacy decision by European Commission
- ↔ SCCs, BCRs, or other transfer mechanisms needed
- ↔ Strong data subject rights attached to transferred data

Data Fiduciary Obligations

Core duties for ALL Data Fiduciaries — and enhanced duties for SDFs

All Data Fiduciaries Must:

- ✓ Implement reasonable security safeguards (organizational + technical)
- ✓ Prevent unauthorized processing, leaks, accidental exposure
- ✓ Notify Data Principals & DPB of personal data breaches
- ✓ Erase personal data once the purpose is fulfilled
- ✓ Maintain effective grievance redressal systems
- ✓ Publish DPO or designated contact on website / app

SDF Appointed Based On:

- Volume & sensitivity of data
- Risk to national interest
- AI profiling & automated decisions
- Public impact & potential harm

Additional SDF Obligations:

- ✓ Appoint India-based DPO (reports to Board)
- ✓ Conduct annual independent audit
- ✓ Annual DPIA (from Nov 2025)
- ✓ Algorithmic risk due diligence
- ✓ Data localisation (if government restricts)

Processor Management & Contracts

Third-party processing does NOT transfer accountability

Data Fiduciary

Instructions only →

Data Processor

⚠ Key Rule

Unlawful outsourcing does NOT eliminate fiduciary accountability

Contractual Obligations Must Define:

Security Controls

Define required technical & organizational safeguards

Storage & Access

Specify where data is stored and who can access it

Breach Notification

Processor must notify DF immediately on discovery

Sub-Processor Management

No sub-delegation without DF's explicit written approval

Exit & Data Return/Deletion

Define process for returning or securely deleting data

Disposal & Sanitization

Certified destruction and proof of erasure required

Risk Management & DPIA

Data Protection Impact Assessment — mandatory for Significant Data Fiduciaries

1

Assess Processing

Map all processing activities — nature, scope, context, purpose

2

Analyze Consequences

Evaluate automated decision-making risks and individual harm

3

Review Controls

Check security safeguards, access controls, encryption

4

Address Minimization

Ensure only minimum data is collected and retained

5

Document Mitigations

Record risk treatment decisions and residual risk acceptance

Risk Model Dimensions

Individual Harm

Direct impact on the data subject — financial loss, discrimination, identity theft

Privacy Risk

Exposure of sensitive data, profiling, surveillance without consent

Systemic & Societal Risk

Algorithmic bias, large-scale processing affecting communities

Public Order & National Security

Data that could undermine sovereignty or be exploited by adversaries

Data Retention & Deletion

Core principle: Purpose Limitation + Storage Minimization

> *"Retain data only as long as the purpose exists. Delete it once the purpose is fulfilled or consent is withdrawn."*

Retain Only for Purpose

Data must not be kept beyond the stated purpose. Once fulfilled, erasure is mandatory.

Consent Withdrawn = Delete

When a user withdraws consent, their data must be erased — including from processors.

Maintain Destruction Logs

Keep auditable records of what was deleted, when, and how for regulatory inspection.

Avoid Blanket Retention

Indefinite retention 'just in case' is explicitly prohibited under DPDP.

Good Practices:

- 📋 Retention Matrix
- 📋 Policy Enforcement Engine
- 📦 Archival Controls
- 🗑 Automatic Deletion Scripts
- ⚠ 48-hr User Notification Before Erasure (Rule 8)

Breach Management

What constitutes a breach and what must you do within 72 hours?

A Breach Includes:

- ! Unauthorized access to personal data
- ! Loss or theft of data
- ! Identity exposure
- ! Modification of data without authorization
- ! Destruction of data
- ! Unauthorized publishing of data

Immediately

First Intimation to DPB

Notify Data Protection Board without delay upon discovery of breach

Within 72 hrs

Detailed Breach Report

Submit comprehensive breach report to DPB with full details

ASAP

Notify Data Principals

Inform affected individuals — nature, impact, and remediation steps

Notification Must Include:

Nature of breach • Categories of data impacted • Remediation steps taken • Further mitigation instructions

Grievance Redressal Mechanism

Every organization must provide a clear, accessible path for complaints

1

Complaint Received

User submits complaint via published grievance channel (website/app)

2

Acknowledge & Track

Organization acknowledges receipt and assigns a tracking reference

3

Human Review

Designated human contact reviews and investigates the complaint

4

Resolve Within 90 Days

Resolution communicated to user within 90-day statutory deadline

5

Escalate if Unresolved

User can approach Data Protection Board (DPB) if unresolved

Organizations Must Ensure:

- Proper channel for user complaints (published on website/app)
- Clear timelines communicated upfront
- Human contact point available (not just bot/automation)
- Escalation to DPO (for Significant Data Fiduciaries)
- Confirmation / communication of resolution to complainant

Data Protection Board (DPB) — Escalation

- If the organization fails to resolve within 90 days, the Data Principal may escalate directly to DPB via the digital complaint portal (operational from Nov 2025).
- DPB has powers to investigate, impose penalties up to ₹250 Cr, and mandate corrective action.

Master Retention Matrix — Quick Reference

Longest applicable period wins. Use this to build your organisation's retention schedule.

RBI — KYC/AML
10 Years
Banking / NBFC / Fintech

SEBI — Broker Records
5–8 Years
Capital Markets / Listed Cos.

IRDAI — Policy Records
3 Yrs + 10 Yr AML
Insurance

PFRDA — NPS Records
Lifetime + 10Y
Pension Funds

Income Tax — Books
8 Years
All taxpaying entities

GST Records
6 Years
All GST-registered entities

MCA / Companies Act
8–10 Years
All registered companies

PMLA — Transaction Recs
10 Years
Banks, FIs, Brokers, Insurers

TRAI — CDR/IPDR
2 Years
Telecom service providers

CERT-In — System Logs
180 Days
All regulated digital entities

Labour — Wages/PF/ESI
3–10 Years
All employers

Healthcare — MCI/ABDM
3–Life Yrs
Hospitals, clinics, pharma

Education — UGC/RTE
5–10 Years
Educational institutions

RERA — Real Estate
5 Yrs post project
Real estate developers

Aadhaar — Auth Logs
6 Months
AUAs / eKYC providers

DPDP Act (Baseline)
Purpose duration + 1 yr logs
ALL Data Fiduciaries

DPO Action: Conflict Resolution & Retention Checklist

What to do when regulations conflict with DPDP — and the DPO's role in each

⚖️ Conflict Resolution Rule: When DPDP purpose-limitation requires erasure but a sectoral law mandates retention → SECTORAL LAW PREVAILS (DPDP Section 8 exemptions apply). The Data Principal's erasure right is blocked by legal retention obligation. DPO must document justification.

01

Identify Applicable Law

Map the data category to all applicable sectoral regulations (RBI, SEBI, IT, Labour etc.)

02

Find Longest Period

Compare all applicable retention periods. The LONGEST period wins and overrides DPDP baseline.

03

Document Legal Justification

Record the legal basis for extended retention. Restrict data use to compliance purpose only.

04

Restrict Further Processing

Data retained beyond DPDP purpose must be ringfenced — no marketing, analytics or profiling allowed.

05

Erase After Maximum Period

Once all applicable retention periods expire, trigger deletion workflow with 48-hr user notification.

DPO Checklist — Retention Policy Governance

- ☑ Map all data categories to applicable regulations ✓
- ☑ Identify longest retention period for each data type ✓
- ☑ Build and maintain a Retention Schedule (matrix) ✓
- ☑ Publish retention periods in Privacy Notice (Rule 3) ✓
- ☑ Implement automated deletion triggers per schedule ✓
- ☑ Establish 48-hour erasure notification workflow ✓
- ☑ Restrict use of compliance-only retained data ✓
- ☑ Log all retention decisions with legal justification ✓
- ☑ Annual review of retention schedule vs regulatory changes ✓
- ☑ SDF: Include retention in annual DPIA & audit scope ✓