



Byte • Patch  
system: online

// DATA PRIVACY BRIEFING

# India Enters Its Privacy Age

Decoding the Digital Personal  
Data Protection Rules, 2025

App & Web Dev + Security



BP

Build secure. Stay compliant. Ship with confidence.

# The DPDP Act, 2023

On 11 August 2023, the President of India formally approved the long-awaited Digital Personal Data Protection Act (DPDPA), 2023.

## Where the Act applies

- Governs the handling of digital personal data inside India — whether gathered online or captured offline and later digitised.
- Also reaches processing done outside India whenever it involves offering goods or services to people located in India.

## Key definitions

- **Personal data** — any information about a person identifiable through it, or in relation to it.
- **Data fiduciary** — any entity that, alone or with others, decides the purpose and means of processing personal data.
- **Significant data fiduciary** — any fiduciary, or class of them, specifically designated by the Central Government.

## Key obligations at a glance

- **Notice** — clear, itemised, plain-language; states the purpose, how to exercise rights, and how to complain to the Board. Available in English or any Eighth-Schedule language.
- **Children's data** — verifiable parental consent required; behavioural tracking and targeted ads aimed at children are barred.
- **Data principal rights** — access, correction & erasure, grievance redressal, and nomination.
- **Transfers outside India** — the Government may list barred territories; some exemptions apply (legal claims, court processing).

## Grounds for processing personal data

### Consent

- Must be freely given, specific and informed.
- Must be unconditional and unambiguous, shown through a clear affirmative act.

### Legitimate uses

- Where the individual has willingly shared their own data.
- Performing a legal duty, or protecting India's sovereignty, integrity or security.
- Issuing any subsidy, benefit, service, certificate, licence or permit.
- Complying with a court judgement, decree or order.
- Responding to a medical emergency that threatens a life.
- Managing an epidemic, disease outbreak or other public-health threat.
- Ensuring safety during a disaster or breakdown of public order.
- For employment, or to shield the employer from loss or liability.

### Penalties for non-compliance

- Fiduciaries failing the provisions — up to **INR 250 crore**.
- A data principal breaching duties — up to **INR 10,000**.
- Failure to report a data breach — up to **INR 200 crore**.
- Failing extra obligations on children — up to **INR 200 crore**.

# What the Rules Cover

The Act was approved on 11 August 2023, but it could only take effect once MeitY issued the supporting Rules. On 3 January 2025, MeitY published the draft DPDP Rules in the Gazette of India, open for public consultation until 18 February 2025.

## 22 Rules

**12** apply directly to data fiduciaries and set out their compliance duties; **7** cover establishing and running the Data Protection Board. The rest address the State and its bodies (**1**) and two further provisions (**2**).

- 1** Greater detail on the notice that must be given to data principals.
- 2** Registration requirements and ongoing duties of the Consent Manager.
- 3** Reasonable security safeguards — both technical and organisational measures.
- 4** Personal-data retention periods tied to the class of data fiduciary.
- 5** A 72-hour window to report a personal data breach to the Board.
- 6** Verifiable consent for a child's data, or that of a person with a disability who has a lawful guardian.
- 7** Relief from certain obligations when processing a child's personal data.
- 8** Extra obligations for Significant Data Fiduciaries (e.g. DPIA, audits).

## 07 Schedules

Four Schedules steer data fiduciaries toward compliance — registering and the duties of a Consent Manager, detailed technical & organisational measures, the grouping of fiduciaries for retention periods, and the categories exempt from children's-data rules. The remaining three relate to how the Board operates.

# Points That Matter

The essential nuances of the Rules every organisation must grasp to stay compliant and safeguard the personal data of its data principals.

01

## Notice & Consent

Check that your privacy notices and consent banners align with the Rules and deliver every piece of required information to data principals.

02

## Verifiable Parental Consent

Put a system in place to confirm genuine consent from a parent or legal guardian before processing the data of a child or person with a disability.

03

## Data Principal Rights

Build clear procedures, contact channels and systems to handle rights requests and run an effective grievance-redressal mechanism.

04

## Consent Manager

Confirm any Consent Manager you appoint meets the Board's conditions and follows the duties set out in the Rules.

05

## Security Safeguards

The Rules prescribe reasonable security measures fiduciaries should adopt to protect personal data and prevent breaches.

06

## Personal Data Breach

Inform affected principals and the Board without delay, with a full report to the Board within 72 hours — facts, circumstances, remedial steps and findings.

07

## Data Retention Timelines

Define how long you keep data before erasing it, based on your class of fiduciary — with specific implications for e-commerce, gaming and social media.

08

## Processor Due Diligence

Apply stronger due diligence when outsourcing to third parties, with thorough agreements spelling out each processor's responsibilities.

09

## Significant Data Fiduciary

Run a DPIA and annual audits, ensure algorithms protect data rights, and observe the limits on transferring data outside India.

# Open Questions

## Significant Data Fiduciaries

The Rules don't define which fiduciaries count as Significant — that comes later from the Central Government after weighing relevant factors.

1

## Consent Manager — internal vs external

Unclear whether a fiduciary may appoint an in-house Consent Manager, whether it needs Board registration or creates a conflict of interest — or if existing mechanisms can continue.

2

## Exemptions for children's data processing

Five categories of fiduciaries and certain purposes are exempt, but it's unsaid whether relief extends to all others not offering child-directed or child-lucrative\* products.

3

## Retrospective consent

No clarity on whether consent gathered before the Act stays valid — whether implied consent with a fresh notice suffices, or explicit purpose-specific consent is needed.

4

## Timeline for rights & grievance redressal

No fixed period for fiduciaries to act on rights requests; firms set their own grievance-redressal response time.

5

## Requirements for cross-border data transfer

No countries or instruments are named yet — the Central Government will specify these by general or special order.

6

## Journalistic exemption

No carve-out for journalists or media, leaving open how duties balance against freedom of expression and the public's right to information.

7

## Exemptions for start-ups

The thresholds — volume, data type, class of fiduciary — for start-ups exempt from notice, DPIA, retention and rights duties are unset.

8

## Restriction on special category of data

The categories of data, and definition of traffic data, subject to cross-border limits for Significant Data Fiduciaries remain unspecified.

9

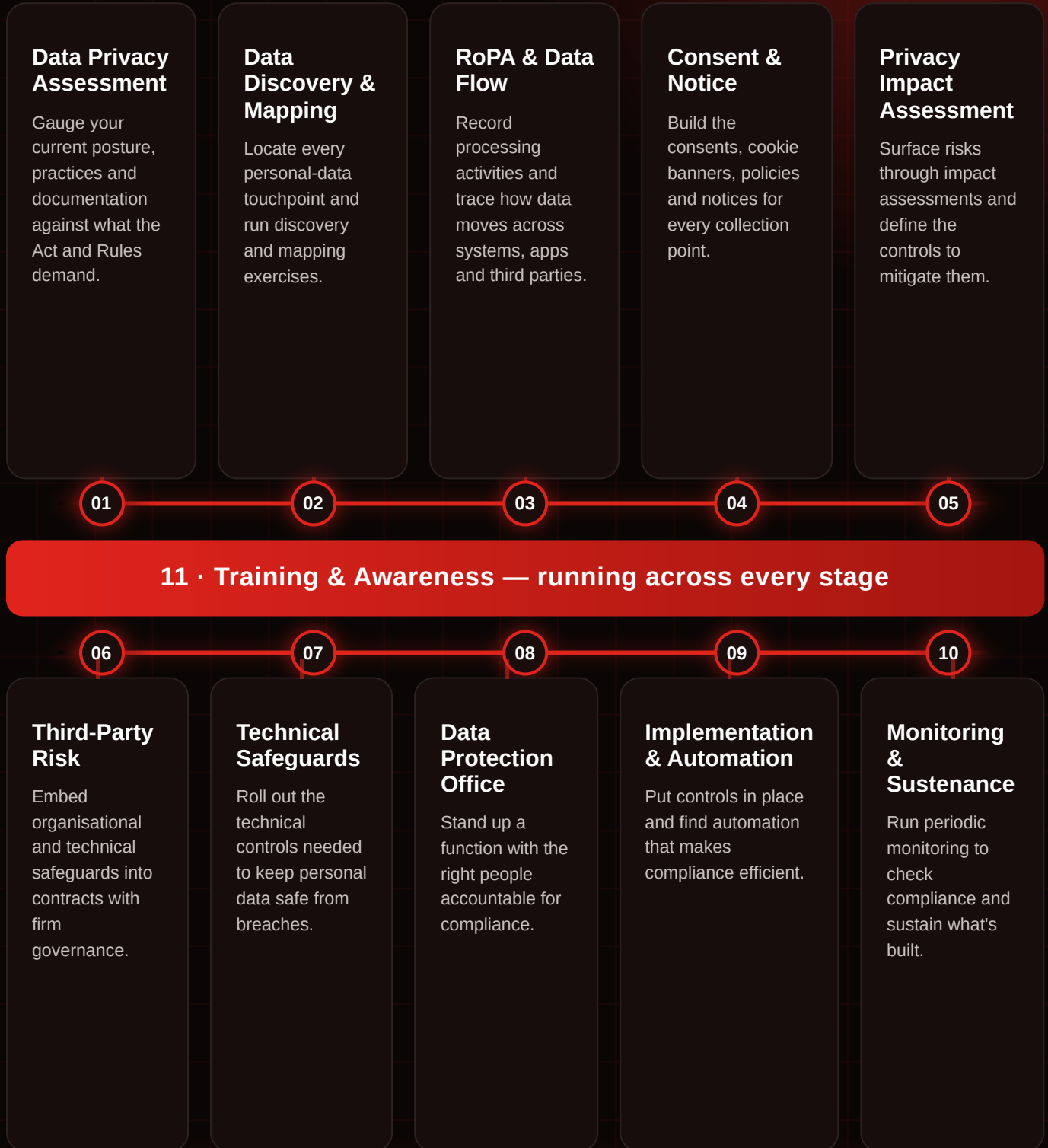
## Breach notification to data principals

Unclear whether every breach must reach the principal, and whether that must happen before the Board is told within 72 hours.

10

# Your Roadmap to Compliance

A complete transformation approach that weaves the Act and its Rules into every stage of your data lifecycle.



BytePatch supports you end-to-end across every stage of this roadmap.

# How We Help You Comply

BytePatch blends product engineering with security expertise, so privacy isn't bolted on at the end — it's built into everything we ship.

## Security

Privacy and security assessments, breach-response readiness, reasonable security safeguards, and the technical controls the Rules expect — built to keep personal data protected.

## Web Dev

Privacy-by-design websites with compliant consent banners, cookie policies, and clear, itemised notices baked into every point where personal data is collected.

## App Dev

Applications engineered with data minimisation, secure storage, retention controls and verifiable-consent flows from day one — never as an afterthought.

## Email

Consent-driven communication so outreach and transactional messages respect each data principal's preferences and the Act's grounds for processing.

## Digital Marketing

Consent-aware campaigns that steer clear of behavioural tracking of children and keep all targeting firmly within the Rules.

Crafted with security, speed & scalability in mind

// GET IN TOUCH

# Let's Build Something Secure

BytePatch Technologies — **Secure. Scale. Ship.** Reach out and we'll turn DPDP compliance into something you ship with confidence.

## Services

### Security

Assessments · safeguards · breach readiness

### Web Development

Privacy-by-design websites

### App Development

Secure, scalable applications

### Email Solutions

Consent-driven, compliant communication

### Digital Marketing

Consent-aware campaigns

## Reach Us

### Mayank Minda

Founder, BytePatch Technologies

### Email

[developer@bytepatch.tech](mailto:developer@bytepatch.tech)

### Phone

+91 98836 53673

### Website

[bytepatch.tech](https://bytepatch.tech)



### Scan to visit

[bytepatch.tech](https://bytepatch.tech)

App & Web Dev + Security

**Secure. Scale. Ship. — let's build something bulletproof together.**



**Byte • Patch**  
Secure. Scale. Ship.

# Building secure software for a privacy-first India

---

BytePatch Technologies builds secure, fast and scalable digital products — across app and web development, security, and digital marketing. Crafted with security, speed and scalability in mind, our work helps businesses ship with confidence while keeping data protection at the core.

Founded by Mayank Minda, BytePatch partners with teams that want privacy designed in from the first line of code — not patched on after launch.

**Disclaimer.** This document is provided in summary form for general information only. It is not a substitute for detailed research or professional legal judgement. BytePatch Technologies accepts no responsibility for any loss arising from anyone acting, or refraining from acting, on the basis of its contents. On any specific matter, please seek advice from a qualified professional. Content adapts publicly available information on the Digital Personal Data Protection Act, 2023 and the draft DPDP Rules, 2025.

© 2026 BytePatch Technologies. All rights reserved. Published in India.