



SILICASECURE
PRIVATE LIMITED

POINT OF VIEW · DATA PRIVACY IN INDIA

A New Era of Privacy in India

The Digital Personal Data Protection Act, 2023 & Rules, 2025

What the law requires, the deadlines that matter,
and how SilicaSecure helps you comply — and prove it.



A decade in the making — now law.

The Supreme Court made privacy a fundamental right in 2017; the DPDP Act was assented on 11 August 2023; and MeitY notified the final DPDP Rules on 13 November 2025. The framework is now operational.

Milestones



WHERE IT APPLIES

- Digital personal data — or data later digitised
- Processing inside India
- Processing outside India when offering goods or services to people in India



WHERE IT DOES NOT

- Personal or domestic processing by an individual
- Personal data made publicly available
- Research, archiving or statistical use (Second Schedule)
- Certain Government processing for sovereignty or security



Process personal data only on a lawful ground.

Either the individual's consent, or one of the specified legitimate uses. Consent must be a genuine, informed choice — and easy to take back.



Key definitions

- Personal data — any data about an identifiable individual
- Data Principal — the person the data is about
- Data Fiduciary — decides why and how data is processed
- Data Processor — processes data for a Fiduciary
- Significant Data Fiduciary — high-volume / high-risk, with extra duties

Lawful basis is the foundation of every processing activity under the Act.



GROUNDS FOR PROCESSING

Consent — must be

- free, specific & informed
- unconditional & unambiguous
- a clear affirmative action
- as easy to withdraw as to give

Legitimate uses — include

- voluntarily provided data
- State subsidy, benefit or licence
- law / sovereignty / security
- compliance with a court order
- medical emergency
- disaster or public-order breakdown
- epidemic / public-health threat
- employment purposes



Clear notice, real rights, strict penalties.

Tell people what you do in plain language, honour their rights, protect children — and know the cost of getting it wrong.

Notice

- Clear, itemised, plain-language
- Purpose, how to exercise rights, how to complain
- English or any Eighth-Schedule language

Children

- Verifiable parental consent first
- No behavioural monitoring of children
- No targeted advertising to children

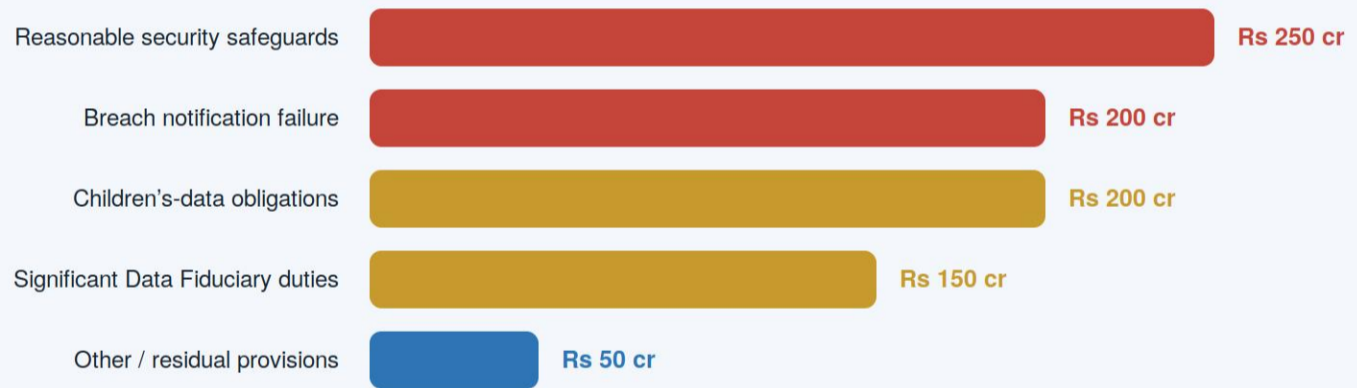
Data Principal rights

- Access to their data
- Correction & erasure
- Grievance redressal
- Nominate another person

Cross-border transfer

- Transfer outside India is allowed
- Subject to Government conditions
- and any restrictions notified

Penalties for non-compliance (maximums)





The Rules make the Act operational.

Of 23 rules, 14 apply directly to Data Fiduciaries. These are the duties every business must build for.



Notice & consent (R3)

- Itemised, plain-language notice
- A link to manage or withdraw consent



Consent Manager (R4)

- Registers with the Board (First Schedule)
- Manages consent securely
- Keeps records for at least 7 years



Security safeguards (R6)

- Encryption, masking, access control
- Activity logging & backups
- At least 1 year of log retention



Personal-data breach (R7)

- Notify principals & Board without delay
- Detailed report to the Board within 72 hours



Retention & deletion (R8)

- Purpose-based erasure timelines
- Keep processing logs \geq 1 year
- 48 hours' notice before deletion



Data Principal rights (R14)

- Published request channels
- Grievance handling within the set time



Children, large players, and the regulator.

Special duties for children’s data and Significant Data Fiduciaries, a retention rule for the largest platforms, and seven schedules of detail.



Verifiable parental consent (R10)

- Verify parent’s identity & the child’s age
- Use ID details or authorised digital tokens



Exceptions (Fourth Schedule)

- Healthcare & allied professionals
- Educational institutions & creches
- Child-transport providers tracking safety



Significant Data Fiduciary (R13)

- Annual DPIA & independent audit
- Algorithmic due diligence
- Report significant findings to the Board



Persons with disability (R11)

- Verifiable consent from a lawful guardian
- Guardianship verified



Three-year deletion for the largest platforms

E-commerce (>2 cr) · online gaming (>50 lakh) · social media (>2 cr) — from last engagement.



The seven schedules

1

Consent Manager eligibility

2

State processing standards

3

Retention timelines by class

4

Children’s-data exemptions

5–6

Data Protection Board terms

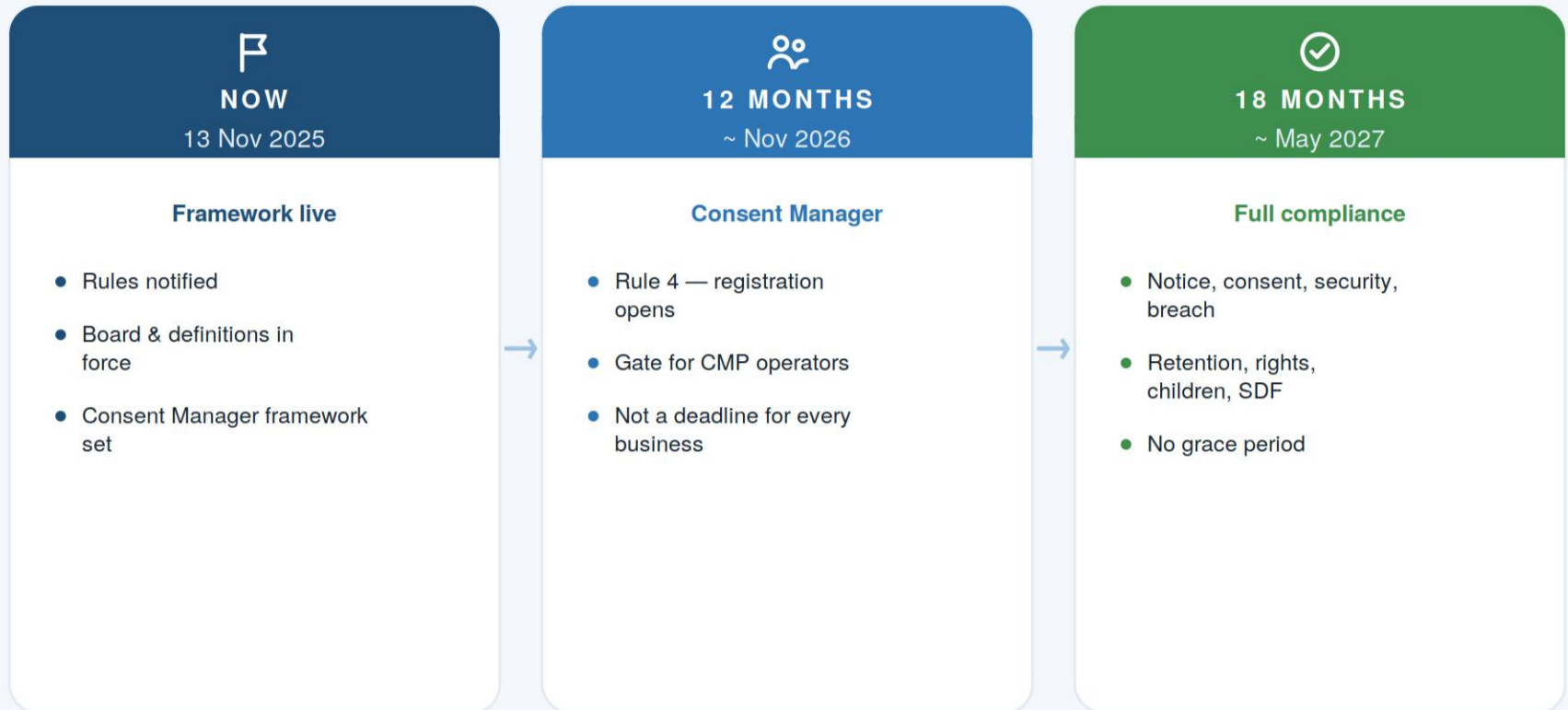
7

Government information requests



Three dates decide your plan.

Obligations switch on in phases from the 13 November 2025 notification. Most businesses must treat ~May 2027 as the hard deadline.



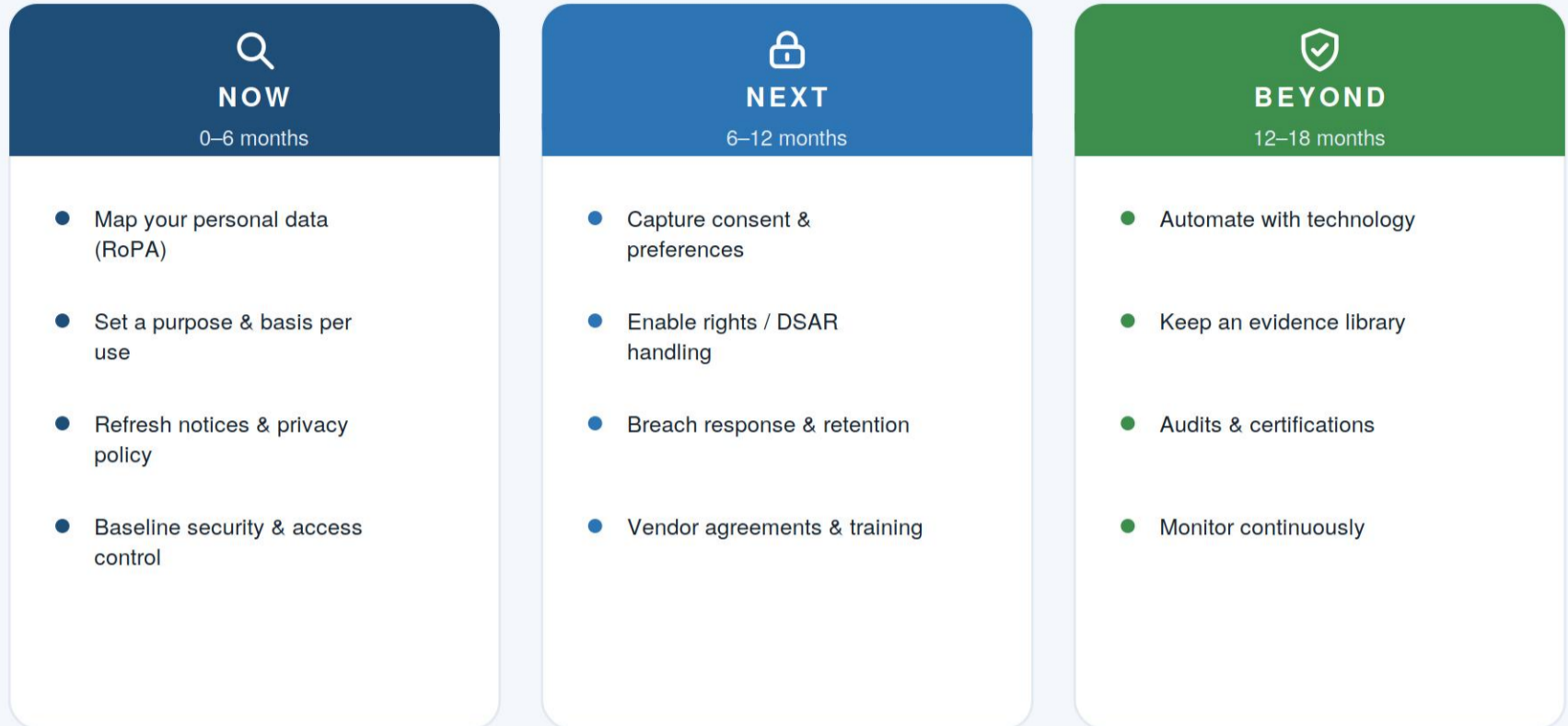
Plan around ~ May 2027

Data mapping, notices, consent tooling and security take months — an early start leaves margin.



A phased path over 12–18 months.

Foundations first, customer-facing controls next, then automation and assurance — so nothing is built on sand.



Compliance is a state to maintain — not a project to finish.

That is why continuous monitoring and provable evidence matter most.



One partner, advisory to technology.

We take you from uncertainty to demonstrable compliance — and keep it provable — with our Consent Management Platform doing the hardest parts automatically.

Assess

Gap assessment vs the Act & Rules

Map

Data discovery, RoPA & data-flow

Lawful basis

A defensible basis & purpose per use

Notice & consent

Compliant, multilingual, provable consent

Rights / DSAR

Access, correction, erasure, grievance

Secure

Encryption, access control, logging

Breach readiness

72-hour Board report & templates

Vendors / DPA

Processor inventory & agreements

Assure

Evidence library & continuous monitoring

Powered by the SilicaSecure CMP

capture · enforce · withdraw · and prove consent



SILICASECURE
PRIVATE LIMITED

WHY SILICASECURE

Compliance you can prove.



Proof, not just promises

Consent in a tamper-evident, independently-verifiable ledger — evidence a regulator can check.



Built in India, for India

India-hosted, multilingual across 22 scheduled languages, aligned to the Consent Manager regime.



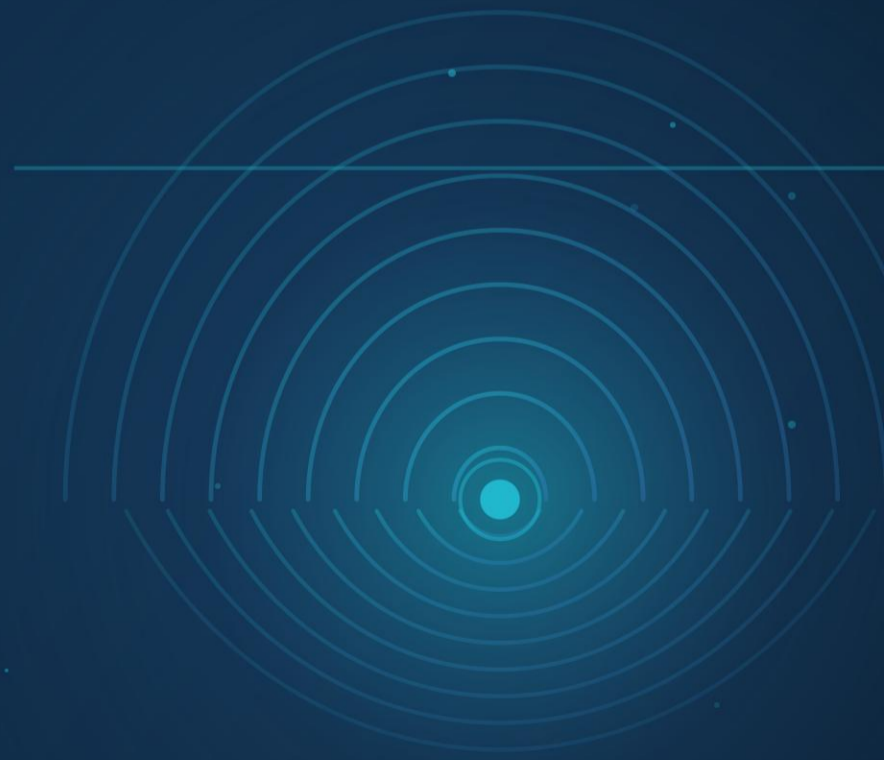
Made for growing businesses

Real compliance for D2C and MSME brands — without enterprise complexity or cost.



A security pedigree

A team with hands-on cybersecurity depth, including a global top-13% finish at HackTheBox.



Talk to us about your DPDP programme

info@silicasecure.com · www.silicasecure.com · +91 90416 50597

A general overview for awareness — not legal advice.