SmartSuite

Framework / Privacy / Global Privacy Regulations

# Digital Personal Data Protection Act, 2023 (DPDPA 2023)

The DPDP Act, 2023 regulates digital personal data in India: consent, Data Fiduciary duties, Data Principal rights, breach intimation and Board penalties up to Rs 250 crore.




## What it is

The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023) is India's data protection statute. Parliament enacted it with the President's assent on August 11, 2023. It governs the processing of digital personal data by Data Fiduciaries, gives Data Principals rights to information, correction, erasure, grievance redress and nomination, and establishes the Data Protection Board of India. Commencement is phased under notifications dated November 13, 2025: the Board and administrative sections at once, Consent Manager registration after one year, and the main obligations after eighteen months, in May 2027.

## At a glance

PUBLISHER
Parliament of India (Rules notified by the Ministry of Electronics and Information Technology)

TYPE
Regulation

VERSION
Act No. 22 of 2023; DPDP Rules, 2025 (G.S.R. 846(E))

EFFECTIVE
Phased from November 13, 2025: Board and administrative provisions at once, Consent Manager registration after one year, main obligations after eighteen months (May 2027)

DOMAIN
Privacy

FAMILY
Global Privacy Regulations

REGION
India

ADOPTION MODEL
Regulatory Compliance

IMPLEMENTATION COMPLEXITY
High

Source: meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf

## Why it matters

- **Consent that can be withdrawn** A Data Principal can withdraw consent at any time, with ease comparable to giving it, and the Data Fiduciary must then cease processing and cause its Data Processors to cease (Section 6(4) and (6)).
- **Rights with defined content** Section 11 gives a summary of the data and the identities of those it was shared with, Section 12 correction, completion, updating and erasure, Section 13 grievance redress and Section 14 nomination.
- **Children and persons with disability** Verifiable consent of a parent or lawful guardian is required before processing, and tracking, behavioral monitoring and targeted advertising directed at children are barred (Section 9).
- **Breach duties** A personal data breach must be intimated to the Board and each affected Data Principal (Section 8(6)), with a 72-hour detailed report to the Board under Rule 7(2)(b).


Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

## How SmartSuite supports DPDP Act 2023

### Processing Inventory and Purposes

Record each category of personal data, its specified purpose, lawful ground (Section 4) and the erasure trigger under Section 8(7) and Rule 8.

### Notice and Consent Records

Keep notice versions and languages, consent and withdrawal events, and the proof the Data Fiduciary must be able to produce under Section 6(10).

### Data Principal Requests and Grievances

Log requests under Sections 11 to 14 and grievances under Rule 14 with owners, due dates inside the ninety-day limit and responses.

### Processor Contracts and Safeguards

Track each Data Processor, its valid contract (Section 8(2)), the Rule 6 safeguards and the one-year log retention.

### Breach Intimation Tracker

Run each breach through the notice to every affected Data Principal and the Board intimation, including the Rule 7(2)(b) 72-hour report.

### Significant Data Fiduciary Assessments

Schedule the annual impact assessment and independent audit (Section 10, Rule 13), the Data Protection Officer role and the report to the Board.

## Common framework mappings

APEC PF | CCPA/CPRA | GDPR | HIPAA | ISO 27701 | NIST Privacy Framework v1.0 | OECD Privacy Guidelines | UK GDPR

## Official resources

### India Digital Personal Data Protection Act (DPDPA) 2023

Provides comprehensive regulations for personal data protection and privacy in India.

meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf

### Digital Personal Data Protection Rules, 2025 (Gazette notification G.S.R. 846(E))

The final DPDP Rules notified on 13 November 2025, with the phased commencement schedule for the Act's obligations.

egazette.gov.in/WriteReadData/2025/267650.pdf

## Frequently asked questions

### Does the DPDP Act apply to companies outside India?

Yes, in part. Section 3(b) applies the Act to processing outside India if it is connected with offering goods or services to Data Principals in India. It also covers digital personal data processed in India, including non-digital data digitized later (Section 3(a)). Processing for personal or domestic purposes is excluded (Section 3(c)).

### When do the DPDP obligations take effect?

Under G.S.R. 843(E) of November 13, 2025, the Board and administrative sections took effect on publication, Consent Manager registration (Section 6(9)) one year later, and Sections 3 to 17 (except Section 6(9)), 27 to 34, 36, 37 and 44(2) eighteen months after publication, in May 2027. The Rules follow the same pattern: Rules 1, 2 and 17 to 21 at once, Rule 4 after one year and Rules 3, 5 to 16, 22 and 23 after eighteen months (G.S.R. 846(E), Rule 1).

### What must a Data Fiduciary do after a personal data breach?

Section 8(6) requires intimation to the Board and each affected Data Principal. Under Rule 7, the Data Principal notice describes the breach, its consequences, mitigation, safety measures and a contact person, without delay. The Board gets a description without delay and a detailed report within seventy-two hours, or a longer period the Board allows in writing (Rule 7(2)).


Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

### What penalties can the Data Protection Board impose?

After an inquiry finding a significant breach, the Board imposes the penalty in the Schedule (Section 33). The maximum is ₹250 crore for failing reasonable security safeguards, ₹200 crore for failing to give breach notice or breaching children's obligations, ₹150 crore for Significant Data Fiduciary duties and ₹50 crore for other breaches. Appeals go to the Appellate Tribunal within sixty days (Section 29).

### What is a Significant Data Fiduciary?

A Data Fiduciary or class notified by the Central Government after assessing factors such as the volume and sensitivity of data and the risk to Data Principals (Section 10(1)). It must appoint an India-based Data Protection Officer and an independent data auditor and carry out periodic impact assessments and audits, which Rule 13 sets once every twelve months, with a report to the Board.

License included / downloadable: Yes The Act and the Rules are Indian law published in the Gazette of India. The texts are free to read on the Ministry of Electronics and Information Technology website.

Full framework page and mappings: smartsuite.com/frameworks/india-digital-personal-data-protection-act-dpdpa-2023