data sutram

A Guide to the DPDP Act & Rules 2025

With the release of the DPDP Rules 2025, India's data protection law becomes fully actionable. The Rules outline how consent, breach reporting, security controls, and data rights must be implemented.

Data Sutram summarises this for teams handling personal data.

November 2025

Table of Contents

Introduction to the DPDP Act	**02**
Key Definitions	**03**
Enforcement Timelines	**04**
Compliance Obligations	**05**
Exemptions	**10**
Penalty Framework	**11**
Practical Roadmap for Businesses	**12**
Responsibility Matrix	**13**

A Quick Overview of the Act

The Digital Personal Data Protection (DPDP) Act, 2023 is India's law for protecting the digital personal data of individuals.

The DPDP Rules 2025 released on 13th November 2025 states how organisations should follow the act and includes steps for consent, security, breach, reporting, retention and individual rights.

Purpose of the DPDP Act:

- To establish a clear legal framework for the protection of digital personal data in India.
- To ensure responsible, lawful and transparent processing of personal data by organisations.
- To give individuals stronger control over their personal data, including consent, access and correction.
- To require businesses to implement reasonable security safeguards to protect data from breaches.
- To create a structured grievance and redressal system for individuals.
- To define clear roles and responsibilities for Data Fiduciaries, Processors, and Consent Managers.
- To introduce a graded penalty framework that encourages compliance and accountability.
- To support India's transition toward a safe, privacy-first digital ecosystem.

The Act is primarily bound to:

Data Principal	Data Fiduciary	Data Processor

Key Definitions (From the Act)

Data Principal

A Data Principal is the individual to whom the data set relates to. In the case of children under 18 years or persons with disabilities, this includes their parents or lawful guardians who can act on their behalf.

Data Fiduciary

A Data Fiduciary is an organisation that decides why and how personal data will be processed.
Examples: Businesses, Platforms, Banks, Fintechs, e-Commerce companies, or Government departments that collect and use personal data.

Data Processor

A Data Processor is an organisation that processes personal data only on behalf of a Data Fiduciary, as per a contract. A processor does not decide the purpose of processing.
Processing includes collection, storage, organisation use, sharing, erasure of any personal data.
The Fiduciary is ultimately responsible for the data.

Key Timelines for the Act

Phase 1

Effective Immediately (13 Nov '25)

- The Data Protection Board of India (DPB) is set up.
- Board's governance and rule-making powers begin.

Phase 2

Effective After 12 Months (Nov '26)

- Framework for Consent Manager registration becomes active. Consent Managers must obtain independent certification and must amend MOA/AOA to embed obligations.
- Technical and operational standards for consent management are introduced.

Phase 3

Effective After 18 Months (May '27)

This is when mandatory compliance begins.

From this date, organisations must follow:

- Notice and Consent Requirements
- Security safeguards
- Breach notifications
- Data principal rights
- Retention and deletion rules
- Cross-border transfer rules
- Significant Data Fiduciary (SDF) requirements.
- Penalties under the Act also become active at this stage.

Time-Phased Enforcement & Registration:

- Consent Manager registration requirements begin after 1 year
- Compliance begins at 18 months

Notice & Consent

Who this applies to:

- Data Fiduciaries

Overview:

- A Data Fiduciary must give a clear, standalone notice before collecting personal data.
- The notice must explain what data is being collected and the exact purpose for which it will be used.
- It must also offer simple options to withdraw consent, exercise rights, and raise complaints with the Data Protection Board.
- The Rules also state that withdrawing consent must be as simple as giving it.

Verifiable Consent for Children

Who this applies to:

- **Data Fiduciaries -** When processing any child's personal data
- **Parents/Guardians -** for providing consent

Overview:

- Before processing a child's personal data, a Data Fiduciary must obtain consent from an adult parent or legal guardian.
- The parent or guardian's identity and age must be verified using reliable information or virtual tokens linked to verified identity details.
- These steps ensure that a child's data is handled only with confirmed, lawful consent.

Obligations of Consent Managers

Who this applies to:

- Consent Managers

Overview:

- Consent Managers must be incorporated in India and have a net worth above ₹2 crore.
- They must operate a secure and accessible digital platform that allows individuals to view, manage, and withdraw consent.
- They must publish required company information, avoid conflicts of interest, and cannot outsource their obligations.
- They must retain records for seven years and maintain a strong audit mechanism, reporting outcomes to the Data Protection Board when required.

Security Safeguards

Who this applies to:

- Data Fiduciary
- Data Processor

Overview:

- Both Data Fiduciaries and Data Processors must implement reasonable security measures to protect personal data.
- These include encryption, masking, access controls, incident detection, and systems to prevent unauthorised access.
- Logs, traffic data, and related information must be retained for at least one year.
- They must also maintain backups and continuity plans to ensure processing is not disrupted.
- Contracts between Fiduciaries and Processors must clearly include these obligations.

Personal Data Breach

Who this applies to:

- All

Overview:

- If a data breach occurs, the Data Fiduciary must inform the Data Protection Board without delay.
- A detailed report must be submitted within 72 hours, outlining the facts, causes, impact, mitigation steps, and notifications made to affected individuals.
- The Fiduciary must also alert impacted individuals as early as possible.
- If the breach occurs at the Data Processor's end, the Processor must immediately inform the Data Fiduciary.

Rights of Data Principals

Who this applies to:

- Data Fiduciary
- Data Principals

Overview:

- Data Fiduciaries must clearly publish how individuals can exercise their rights and the relevant contact details (including the DPO for SDFs).
- Individuals can request access to their data, seek correction or updation, request erasure, raise grievances (which must be resolved within 90 days), and nominate someone to act on their behalf.

Data Retention and Erasure

Who this applies to:

- Data Fiduciaries
- Data Processors
- Certain specified Fiduciaries

Overview:

- Personal data must be deleted after the purpose is fulfilled, unless the law requires it to be kept longer.
- Before deletion, the Fiduciary must check if the individual has engaged again or exercised their rights.
- Certain large platforms (e-commerce, social media intermediaries, or gaming platforms with two crore+ users) must retain data for three years and notify individuals 48 hours before deletion.
- All processing logs must be kept for at least one year.

Significant Data Fiduciaries (SDFs)

Who this applies to:

- Significant Data Fiduciaries

Overview:

- The government may classify certain Data Fiduciaries as SDFs based on factors like volume or sensitivity of data.
- SDFs must conduct annual Data Protection Impact Assessments, undergo independent audits, and review algorithms used in processing.
- They must appoint a Data Protection Officer and publish their contact details prominently.
- They must also follow any cross-border transfer rules notified by the government.

Cross-Border Data Transfers

Who this applies to:

- Data Fiduciaries
- Data Processors

Overview:

- Personal data can be transferred outside India unless the Central Government issues a notification restricting specific countries, entities, or categories of transfers.

Exemptions Under the DPDP Act 2025

The DPDP Act allows the Central Government to grant exemptions for specific situations where applying all obligations of the Act may not be practical or necessary. These exemptions are narrowly framed and are meant to support national security, law enforcement, research, and certain public-interest functions.

Types of Exemptions:

- **Government Notified Exemptions:** The government may exempt any instrumentality of the State from specific provisions for reasons such as national security, public order, or preventing offences.
- **Research, Archiving & Statistical Purposes:** Personal data processed purely for research, archiving, or statistical purposes may be exempt from obligations like consent, retention rules, or data principal rights provided the processing is non-commercial and follows privacy safeguards.
- **Enforcement & Legal Proceedings:** Processing personal data for preventing, detecting, investigating, or prosecuting offences may receive exemptions from notice, consent, or erasure requirements.
- **Employment-Related Purposes:** Certain HR and employment-related processing may be exempt, such as recruitment, termination, benefits, and attendance where strict notice/consent structures may not always apply.
- **Specific Classes of Fiduciaries:** The government can exempt small entities, startups, or specific categories of organisations from some obligations, depending on risk and scale of processing.

Conditions:

Even when exemptions apply, organisations must:

- restrict processing to the specific notified purpose
- ensure data is not misused or processed beyond what is necessary
- maintain reasonable safeguards where possible

Penalities

The Act provides a structured system of penalties for failures related to consent, security, breach reporting, and other obligations.

The exact penalty depends on the category and seriousness of the breach.

Upto ₹ 250 crore

for failure to implement required security safeguards

Upto ₹ 200 crore

for failure to report data breaches

Upto ₹ 200 crore

for violations related to consent and notice

Upto ₹ 150 crore

for not meeting SDF obligations

Upto ₹ 50 crore

for other violations under the Act

Upto ₹ 10,000

On Data Principal for breach of their duties (eg. filing a false complaint)

Practical Compliance Roadmap for Businesses

As the DPDP Act's obligations come into force, organisations need to put in place a clear and actionable plan to meet compliance requirements. Below is a straightforward roadmap to help businesses get started.

1. **Identify & Classify Personal Data:** Map the personal data you collect, where it sits, why it is needed, and which teams use it. Categorise data by purpose and sensitivity to understand your exposure.
2. **Review Consent & Notice Flows:** Evaluate all points where you request personal data. Ensure notices are complete, easy to understand, and independent. Remove vague language and ensure consent can be withdrawn easily.
3. **Refresh Privacy Documentation:** Update your privacy policy in simple language. Make sure it includes DPDP-required information such as purposes, rights, grievance formats, and withdrawal mechanisms.
4. **Strengthen Security Measures:** Assess your current technical and organisational safeguards. Implement encryption, access control, monitoring, breach-detection tools, and other reasonable security practices.
5. **Set Up a Breach Response Framework:** Create a clear internal playbook for identifying, assessing, and reporting breaches. Define how to notify the Data Protection Board and affected individuals within required timelines.
6. **Train Teams & Define Ownership:** Educate all employees handling personal data on their responsibilities. Assign owners for notices, rights requests, breach responses, and vendor management.
7. **Prepare for SDF Obligations (if applicable):** If you are likely to be designated as a Significant Data Fiduciary, start preparing for DPIAs, annual audits, algorithm evaluations, and appointing a dedicated Data Protection Officer.
8. **Align Vendors & Contracts:** Review agreements with all Data Processors. Ensure contracts clearly define processing instructions, security expectations, and breach-notification timelines.
9. **Establish Retention & Deletion Practices:** Define how long data will be stored and set up deletion workflows once the purpose is complete. For large platforms, plan for mandatory retention windows and user notifications before deletion.

Summary for Data Fiduciaries vs Data Processors

Area	Data Fiduciary	Data Processor
Purpose of processing	Decides	Does not decide
Processing rights	Full responsibility	Only as per contract
Breach reporting	Must inform DPB + individuals	Must inform Fiduciary
Notices & consent	Must provide	Not applicable
Rights requests	Must enable	Support through contract
Security	Must implement	Must implement
Retention & erasure	Responsible	Follows instructions
DPIA, audits, DPO	Only if SDF	Not applicable

About Data Sutram

Data Sutram is a RegTech company building India's first full-scale Identity Bureau — an unified data intelligence that powers fraud, identity, and contactability solutions for enterprises at scale. The DS Platform processes signals from 250+ data sources, to create a 360° intelligence layer for smarter onboarding, better underwriting, and proactive portfolio monitoring.

DS Trust | DS Profile | DS Resolve

Book A Demo