India’s Digital Personal Data Protection Act, 2023: A White Paper for Founders, Compliance Leads, and Advisers

Navneet

17 November 2026

Disclaimer. This paper is general information and is not legal advice. Facts are stated as of 17 November 2026 and rest on the official texts listed in the References.

Abstract

India’s Digital Personal Data Protection Act, 2023 (DPDP Act) is the country’s first general law on personal data. It applies to any business handling digital personal data in India and to foreign businesses offering goods or services to people in India. This paper explains, in plain language, the Act’s background, scope, roles, grounds for processing, fiduciary duties, individual rights, significant fiduciary and cross-border provisions, exemptions, and enforcement. It summarises the Digital Personal Data Protection Rules, 2025 and their phased timeline, under which the core duties begin on 13 May 2027. A government proposal to shorten that window had not been notified as of 16 November 2026. The paper compares the Act with the EU General Data Protection Regulation (GDPR) and the earlier IT Act rules, outlines sector and size effects, and proposes a 14-week readiness roadmap for small and mid-size businesses. It concludes that the sensible course is to map data, fix notice and consent first, and keep dated records as evidence of reasonable effort.

Keywords: DPDP Act 2023, DPDP Rules 2025, data protection, data fiduciary, consent, India, compliance

Executive Summary

The DPDP Act is built on one idea: personal data should be used only for a stated purpose, with the person's clear consent or a narrow legal reason, and it must be protected (Digital Personal Data Protection Act, 2023). Businesses, called Data Fiduciaries, must give a plain notice, collect only what they need, keep data safe, report breaches, delete data when it is no longer needed, and answer people's requests. Penalties reach ₹250 crore per breach. The core duties start on 13 May 2027 (Ministry of Electronics and Information Technology [MeitY], 2025), so the practical window to prepare is about six months from the date of this paper.

Five actions should come first. (1) Map the data: list what personal data is collected, why, where it is stored, and which vendors touch it. (2) Fix notice and consent: publish an itemised notice and make consent specific and as easy to withdraw as to give. (3) Secure the data with reasonable safeguards and keep logs for at least one year. (4) Prepare for breaches and requests, including a breach plan with a report to the Board within 72 hours and a process for access, correction, and erasure requests. (5) Sign valid contracts with vendors, because a fiduciary remains responsible for its processors.

The government has discussed shortening the compliance window, but as of the latest source checked, no change has been notified (see Section 10).

1. Background and Purpose

The DPDP Act exists because privacy in India moved from a policy idea to a protected right, and the older rules were too thin for a digital economy. Until 2023, the main rules were Section 43A of the Information Technology Act, 2000 and the 2011 "SPDI" Rules. They covered only a short list of sensitive data and applied mainly to companies, so most everyday data use had no clear standard. In 2017 the Supreme Court held in *Justice K.S. Puttaswamy v. Union of India* that privacy is a fundamental right. That ruling pushed the government to draft a full law, after earlier bills in 2018, 2019, and 2022.

Parliament passed the Act in August 2023. It is short and principle-based: it states duties and rights and leaves detail to Rules. The Digital Personal Data Protection Rules, 2025 were notified on 13 November 2025 and supply that detail (MeitY, 2025). The Act has a two-sided purpose: to protect the right of people to their personal data, and to allow lawful processing for legitimate purposes. In practice, it tries to protect individuals without making ordinary business impossible.

2. Scope and Key Definitions

The Act covers digital personal data and reaches further than many businesses expect. Under Section 3 it applies to personal data processed in India, whether it was collected digitally or collected on paper and later digitised, and to processing outside India that is connected to offering goods or services to people in India. It does not apply to personal or domestic use, such as an address book kept for family, or to data that the person made public or that a law requires to be made public (Digital Personal Data Protection Act, 2023).

Table 1
Key Terms in the DPDP Act

Term	Meaning in the Act
Personal data	Any data about an individual who is identifiable by or in relation to that data. The Act has no separate “sensitive” category.
Processing	Any operation on the data: collecting, storing, using, sharing, or deleting it.
Child	Anyone under 18.
Data Fiduciary	The party that decides why and how personal data is processed. Closest to a “controller”.
Data Processor	A party that processes data on a fiduciary’s behalf. Closest to a “processor”.
Data Principal	The individual the data is about. For a child or a person with a disability, this includes the parent or lawful guardian.

Two features stand out. The Act applies to any size of business, from a corner shop with a web form to a multinational. And because there is no “sensitive data” tier, a customer’s email address and a medical record fall under the same core rules; the Act and Rules add extra duties for children and for large “significant” fiduciaries instead.

3. Roles Under the Act

Six roles do most of the work, and knowing which one a business holds shows which duties apply (Table 2). A useful test is this: if a business decides what data a form asks for and why, it is a fiduciary. If it only stores or processes data on someone else’s instructions, such as a payroll vendor or a cloud host, it is a processor for that client, but still a fiduciary for its own staff and customers.

Table 2
Roles Under the DPDP Act

Role	What it does	Why it matters
Data Principal	The person whose data it is.	Holds the rights described in Section 6.
Data Fiduciary	Decides why and how data is used.	Carries almost every duty and is liable for its processors.
Significant Data Fiduciary (SDF)	A fiduciary the government designates, based on data volume and sensitivity, risk to people, and national interests.	Faces extra duties: an India-based Data Protection Officer, an independent auditor, and impact assessments.
Data Processor	Handles data for a fiduciary under a contract.	Has no direct duties of its own in the Act, but the fiduciary answers for it.
Consent Manager	A registered platform that lets a person give, review, and withdraw consent in one place.	Must act in the person's interest and be "data-blind". Registration opens 13 November 2026.
Data Protection Board	The enforcement body.	Investigates breaches, directs fixes, and imposes penalties. It works as a digital office.

4. Grounds for Processing: Consent and Legitimate Uses

A fiduciary may process personal data only in two situations: the person has given valid consent, or the use falls within a list of "legitimate uses" (Digital Personal Data Protection Act, 2023).

4.1 Consent (Section 6)

Valid consent must be free, specific, informed, unconditional, and unambiguous, and given by a clear action such as ticking a box. Four consequences follow. First, consent is limited to the purpose: it covers only the data needed for the stated purpose, so bundling unrelated uses into one tick-box is not valid. Second, withdrawal must be about as easy as giving consent, and the Rules expect a visible link or similar means; past processing stays lawful. Third, the fiduciary carries the burden of showing that notice was given and consent obtained, so records matter. Fourth, a notice must come first, itemising the data, the purposes, and the goods or services enabled, and it must stand apart from other terms. Consent can also be given through a registered Consent Manager.

4.2 Legitimate Uses (Section 7)

Some processing needs no consent. The main cases are: a person voluntarily gives data for a stated purpose and does not object to its use; the State provides subsidies, benefits, licences, or services; compliance with a law, court order, or judgment; responding to a medical emergency, an epidemic, or a disaster; and employment, where processing is needed for employer duties such as payroll and safeguarding against loss or liability. Because this list is narrow, most commercial uses, including marketing and analytics, depend on consent. Businesses should not stretch the list to avoid consent.

5. Duties of Data Fiduciaries

Section 8 and the Rules turn the principles into a working list of duties that apply whether or not the business is large (Table 3).

Table 3
Duties of Data Fiduciaries

Duty	What it means in practice
Notice	Tell people, in plain language, what data is collected, why, what it enables, how to withdraw consent, how to complain, and how to reach the Board.
Accuracy	Keep data complete and accurate if it is used to make decisions about a person or shared with others.
Security	Use reasonable safeguards: access control, monitoring, continuity measures, and logs kept for at least one year. The Rules set no named standard.
Breach reporting	Tell the Board without undue delay, then send a detailed report within 72 hours (the Board can extend this). Tell affected people without delay.
Erasure and retention	Delete data when consent is withdrawn or the purpose is served, unless a law requires keeping it.
Processors	Use a valid contract with every processor and remain responsible for what it does.
Contact point	Publish the contact details of a person who can answer questions about data use.
Grievances	Run a grievance process and respond within a reasonable time, which the Rules cap at 90 days.

5.1 Children

Anyone under 18 is a child. Before processing a child’s data, a fiduciary needs verifiable consent from a parent or guardian and must check that the person giving it is an identifiable adult. The Act bans processing that could harm a child’s well-being, and bans tracking, behavioural monitoring, and targeted advertising aimed at children. The Rules exempt some settings, such as clinics, schools, and childcare, for specified purposes.

5.2 Retention Caps for Large Platforms

The Rules add a fixed limit for the largest consumer platforms: e-commerce and social media services with 2 crore (20 million) or more users in India, and online gaming services with 50 lakh (5 million) or more. These must delete personal data after three years of inactivity, after giving the person 48 hours' notice. For some public-interest purposes, the Rules also require keeping personal data, traffic data, and logs for at least one year (Rule 8(3)); deletion duties do not override this.

6. Rights of Data Principals

People hold four rights over their data, plus duties of their own (Table 4). A business must be able to act on a request, so each right needs a named owner and a process.

Table 4
Rights of Data Principals

Right	What a person can ask for	Section
Access	A summary of the data held, what is done with it, and who it was shared with.	11
Correction and erasure	Correct, complete, or update their data, or have it erased when it is no longer needed.	12
Grievance redress	A response to a complaint through the fiduciary's grievance process.	13
Nomination	Name someone to exercise their rights if they die or cannot act.	14

The Act does not include a right to data portability or a right to object to automated decisions, which the GDPR does. It also expects people to try the grievance process before going to the Board, so a working process protects the business as well as the customer. People also have duties under Section 15: they must not impersonate others, file false complaints, or give false information when asking for a correction. Breaking these can lead to a penalty of up to ₹10,000.

In practice, a business should build a single intake point for requests (a form and a monitored mailbox), log the date each one arrives, verify the requester's identity, track the response against its own deadline, and close each request with a dated reply kept on file.

7. Significant Data Fiduciaries and Cross-Border Transfers

7.1 Significant Data Fiduciaries

The government can designate a fiduciary as “significant” (Section 10) after considering the volume and sensitivity of the data, the risk to people’s rights, the risk to the State’s sovereignty and security, and the effect on electoral democracy. Designation is not tied to company size alone. A significant fiduciary must appoint an India-based Data Protection Officer who reports to its board or equivalent, appoint an independent data auditor, run an annual data protection impact assessment and independent audit and send the Board a report of significant findings, and check that its algorithmic and technical tools do not harm people’s rights.

7.2 Cross-Border Transfers

The Act takes an open approach to moving data abroad (Section 16). A transfer is allowed unless the government restricts it to a specific country or territory by notification. This is a “negative list” model, unlike regimes that require each transfer to qualify first. Two cautions apply. First, other Indian laws that set stricter localisation or protection rules, such as sector rules from regulators, continue to apply. Second, the Rules let the government impose conditions where foreign states or entities under their control could gain access to data, and let it require significant fiduciaries to keep specified categories of data in India. No notified country-level restriction list was found for this paper.

8. Exemptions

Section 17 lists situations where some or all duties fall away, and most small businesses will meet only a few of them (Table 5). The government can also exempt classes of fiduciaries by notification within five years of the Act’s commencement. Exemptions differ in reach, so Section 17 should be read for the exact duties each one lifts.

Table 5
Main Exemptions Under Section 17

Exemption	Typical case
Legal rights and claims	Enforcing a legal right, or a court or tribunal order.
Crime and security	Preventing or investigating offences.
Foreign contracts	Processing data of people outside India under a contract with a foreign party, for example an Indian outsourcing firm.
Mergers and restructuring	Approved schemes of arrangement.
Loan default checks	Finding assets or tracing defaulters by financial institutions.
Research, archiving, statistics	Allowed if the data is not used to make decisions about a person and the Rules' safeguards are met.
Notified startups and other classes	The government may exempt certain data fiduciaries or classes, including startups, from some duties.
State instrumentalities	Notified agencies, on grounds such as security and public order.

9. Enforcement and Penalties

The Data Protection Board enforces the Act, and the maximum penalty for a single breach is ₹250 crore. The Schedule to the Act sets the ceilings shown in Table 6. These are ceilings, not fixed amounts: the Board sets the figure after weighing the nature, gravity, and length of the breach, the type of data, whether it repeated, any gain or loss, and what the business did to fix it.

Table 6
Maximum Penalties Under the Schedule

Breach	Section	Maximum penalty
Failing to take reasonable security safeguards	8(5)	₹250 crore
Failing to notify the Board and people of a breach	8(6)	₹200 crore
Failing child-specific obligations	9	₹200 crore
Failing significant fiduciary obligations	10	₹150 crore
Any other breach of the Act or Rules	None specific	₹50 crore
Breaching a voluntary undertaking	32	Up to the penalty for the original breach
A person failing their own duties	15	₹10,000

9.1 How a Case Moves

A person first complains to the business and uses its grievance process. If the matter is unresolved, the person (or the government, a court, or the business itself on a breach) refers it to the Board. The Board inquires, can order interim measures, and can accept a voluntary undertaking from the business, which ends proceedings on that point. It may refer a dispute to mediation or impose a penalty after a hearing. A party can appeal to the Appellate Tribunal (TDSAT) within 60 days. Penalties are paid to the government; the Act gives individuals no right to compensation, which is a notable difference from the GDPR. Because the Board weighs the factors above, records of notice, consent, safeguards, and the handling of each request are the best evidence of reasonable effort.

10. The DPDP Rules 2025 and the Timeline

The government notified the Digital Personal Data Protection Rules, 2025 on 13 November 2025 and set a phased start, so different parts of the law switch on at different dates (MeitY, 2025). The third phase switches on notice, consent, security safeguards, breach reporting, erasure, children’s data, significant fiduciary duties, and the Board’s remaining powers. Until then, Section 43A of the IT Act and the 2011 SPDI Rules stay in force, as does Section 72-A on wrongful disclosure.

10.1 What the Rules Add

The Rules add an itemised notice describing the data, the specific purposes, and the goods or services enabled, shown apart from other terms; registration and conduct rules for Consent Managers, which must avoid conflicts of interest and not read the data passing through them; a first breach alert to the Board without undue delay and a detailed report within 72 hours; verifiable parental consent with checks that the parent is an identifiable adult; an annual impact assessment and audit for significant fiduciaries; log retention of at least one year and a three-year inactivity limit for the largest platforms; a 90-day cap on grievance responses; and a government power to set conditions on cross-border transfers.

10.2 A Proposal to Shorten the Window

In early 2026 the government discussed cutting the 18-month period to 12 months, which would have brought the core duties forward to 13 November 2026 and started some significant-fiduciary and cross-border measures sooner. Reports describe this as a proposal that went to industry for comment in February 2026 (S.S. Rana & Co., n.d.). As of 16 November 2026, no notified change was found, so 13 May 2027 stands. Businesses should check the Gazette of India before relying on a date.

11. Comparison with the GDPR and the Earlier IT Act Rules

The DPDP Act is shorter and simpler than the EU's GDPR and much broader than the rules it replaces. Table 7 is general and simplified.

Table 7
Comparison of the DPDP Act, the GDPR, and the IT Act Rules

Topic	DPDP Act 2023	GDPR (EU)	IT Act s43A and SPDI Rules 2011
Data covered	All digital personal data	All personal data; paper files too if filed	A short list of "sensitive" data
Who is covered	Any business or person	Any controller or processor	Bodies corporate
Legal grounds	Consent or listed legitimate uses	Six grounds, including contract and legitimate interests	Written consent for sensitive data
Sensitive data tier	None	Yes (special categories)	Yes
Individual rights	Access, correction, erasure, grievance, nomination	Also portability, objection, limits on automated decisions	Access and correction
Children	Under 18, parental consent	Under 16 (states may lower to 13)	Not addressed
Breach reporting	Board and people; 72-hour detailed report	Authority within 72 hours; people if high risk	No duty in these rules
Cross-border	Allowed unless a country is restricted	Needs a transfer mechanism	Conditions on transfer
Compensation to people	None in the Act	Yes	Through adjudication
Top penalty	₹250 crore	Higher of €20 million or 4% of turnover	Compensation set by an adjudicating officer

Note. The GDPR and IT Act columns, and the court ruling in Section 1, are general knowledge and were not re-checked against a source for this paper.

Three differences matter most for Indian businesses. There is no "legitimate interests" ground, so consent does more work than under the GDPR. The Act treats all personal data alike, so teams cannot lighten duties by arguing data is not "sensitive". And the 72-hour breach report applies to every notifiable breach, not only high-risk ones. A business already compliant with the GDPR has a head start but not a finished job, since India's rules on consent wording, children's data, and the Board process need separate work.

12. Impact by Sector and Business Size

The duties are the same for everyone, but the hard part differs by sector and by size (Table 8).

Table 8
Where the Work Concentrates by Sector

Sector	Where the work concentrates
E-commerce and retail	Consent on checkout and marketing, vendor sprawl (payments, logistics, ads), and the three-year inactivity limit for the largest platforms.
Fintech and banking	Sector regulator rules still apply on top. Breach reporting, retention, and consent records are the main gaps.
Healthcare	Patient records are high risk. Clinics get some child-data exemptions, but security safeguards matter most.
Education	Mostly children's data, so parental consent and a ban on tracking and targeted ads. Schools get specified exemptions.
SaaS and IT services	Often a processor for clients and a fiduciary for its own users. Contracts, sub-processors, and the foreign-contract exemption need care.
Media and gaming	Large user bases and children. Higher chance of significant fiduciary designation and the inactivity limit.
HR and staffing	Employment is a legitimate use, but only for what the job needs. Candidate data still needs notice.

By size, solo and micro businesses will find that notice, consent wording, a contact point, and basic security cover most of the work, although a website form and a spreadsheet of customers are in scope. Small and mid-size companies mainly need a vendor register, a breach plan, and a request process, and few will be designated significant. Large and designated firms face a data protection officer, independent audit, impact assessments, and possible limits on where data is stored. The Rules give startups no blanket relief; the Act lets the government exempt notified classes of startups from some duties, but none was identified in the sources checked for this paper.

13. A Practical Readiness Roadmap

As a rough guide, a small or mid-size business could cover the steps in Table 9 in about 14 weeks of steady work, which would leave a buffer before 13 May 2027. Larger firms should plan for longer. A dated record of each step is the best evidence of reasonable effort if something goes wrong.

Table 9
Fourteen-Week Readiness Roadmap

Weeks	Step	Key actions
1–2	Map and decide	List every place personal data is collected (forms, apps, emails, paper), what each field is for, where it is stored, and which vendors see it. Name an owner for privacy.
3–4	Notice and consent	Write an itemised notice. Rewrite every consent prompt so it is specific, separate from other terms, and easy to withdraw. Add consent records.
5–7	Security and logs	Check access control, encryption in transit and at rest, backups, and monitoring. Keep logs for at least one year. Fix the affordable gaps now.
8–9	Vendors	Build a register of processors. Add contract clauses on purpose limits, security, breach alerts, deletion, and sub-processors.
10–11	Breach and requests	Write a breach plan with roles and the 72-hour report. Set up intake, identity checks, and tracking for access, correction, and erasure requests, with a 90-day maximum.
12	Children and retention	Decide whether children’s data is processed. If so, add parental consent and remove tracking and targeted ads. Set retention periods and a deletion routine.
13–14	Train and test	Brief staff, run a breach drill, and test one request end to end.
Then	Keep it alive	Review notices when adding a tool, re-check vendors yearly, and re-scan the site after each major change.

14. Open Questions and What to Watch

Several points are not settled, and a prudent plan keeps room for them. The first is the compliance date: whether the government will shorten the window should be watched through the Gazette of India and MeitY. The second is who will be designated significant; the Act sets factors but no list, and large platforms, financial firms, and firms with big or sensitive datasets should expect to be considered. The third is cross-border limits: which countries, if any, will be restricted, and what significant fiduciaries must keep in India, is still to be notified.

Fourth, sector overlap remains. Regulators such as the RBI, SEBI, and IRDAI have their own data rules. Section 38 says the Act adds to other laws and prevails in a conflict, while Section 16 keeps stricter transfer rules, so firms in these sectors need to map both. Fifth, Consent Manager registration opened on 13 November 2026, and how many will register, how fiduciaries will connect to them, and whether people will use them is unknown. Sixth, the Board’s enforcement style, its first orders, and its use of voluntary undertakings will set real expectations once the core duties start. Finally, some detail is unclear, such as how to prove consent for existing customers whose data was collected before the Act, and how the legitimate-use ground for voluntarily given data will be read. A good habit is to review official sources monthly until the core duties start and to date-stamp every compliance decision.

Conclusion

The DPDP Act asks businesses to do a small number of things well: say plainly what data they use and why, get clear consent, keep the data safe, report breaches, and answer people’s requests. The duties are simple to state and take real work to prove. With core duties starting on 13 May 2027, the sensible path is to map data now, fix notice and consent first, and build the paper trail as it goes. Any announcement of a shorter timeline should be treated as a reason to move faster, not as a surprise.

References

Digital Personal Data Protection Act, 2023. (n.d.). India Code.

Digital Personal Data Protection Act, 2023. (n.d.). Ministry of Electronics and Information Technology (MeitY).

Ministry of Electronics and Information Technology. (n.d.). *Ministry of Electronics and Information Technology*. Government of India.

Ministry of Electronics and Information Technology. (2025). *Digital Personal Data Protection Rules, 2025*. Government of India.

Mondaq. (n.d.). *Digital Personal Data Protection Rules 2025: Highlights*.

Legal 500. (n.d.). *The privacy timer starts now: The DPDP Rules and the 18-month countdown*.

Press Information Bureau. (n.d.). *Press release on the Digital Personal Data Protection Rules*. Government of India.

Press Information Bureau. (n.d.). *Explainer on the Digital Personal Data Protection Rules* [PDF]. Government of India.

S.S. Rana & Co. (n.d.). *MeitY plans to cut short DPDP compliance timeline*.

Notes on sources. The India Code text of the Act and the three commentary pieces were opened for this paper. The Rules PDF and the PIB pages are official but were not opened here; rule numbers and exact figures should be confirmed there. Publication dates and URLs for several entries are marked n.d. or omitted and should be added from the originals before formal submission. The exemptions beyond the Act's own text are general knowledge and were not re-checked.