DPDP SERIES FOR BUSINESSES

The DPDP Act for a business, in plain words

What it asks of you, and by when. Main duties apply from 13 May 2027.



Mukul Nimrani & Co., Practising Company Secretaries, Lucknow

October 2026 | General information, not legal advice

Meet Myasha

Who this is for: owners and directors of small and mid-sized businesses.

What you get: the whole law on a few slides, a plan for the next seven months, and a list of first steps.

What it is not: legal advice. Read the official Act and Rules, or take advice on your facts, before you act.

Want more detail? The full series is on our website: a main guide and four parts.



MYASHA EXPLAINS

Hello! Laws love short forms: DPDP, DPB, SDF, DPO.

Wherever a strange word turns up, I will explain it in one or two lines.

The law in one minute

Two texts: the Digital Personal Data Protection Act, 2023 and the DPDP Rules, 2025 (G.S.R. 846(E), 13 November 2025).

The core idea: use a person's data only with her consent, or for a use the law allows without asking.

The duties: tell people, keep data safe, report leaks, delete what you no longer need, answer requests.

The referee: the Data Protection Board can impose penalties of up to ₹250 crore.

No size limit: a five-person firm with a customer list in Excel is covered.



MYASHA EXPLAINS

DPDP is short for Digital Personal Data Protection. It is the law on how businesses must treat information about people.

Three words you need first

Data Principal
The person the data is about: your customer, your employee

Data Fiduciary
Your business: it decides why and how the data is used

Data Processor
A vendor handling data for you: payroll, cloud host, call centre

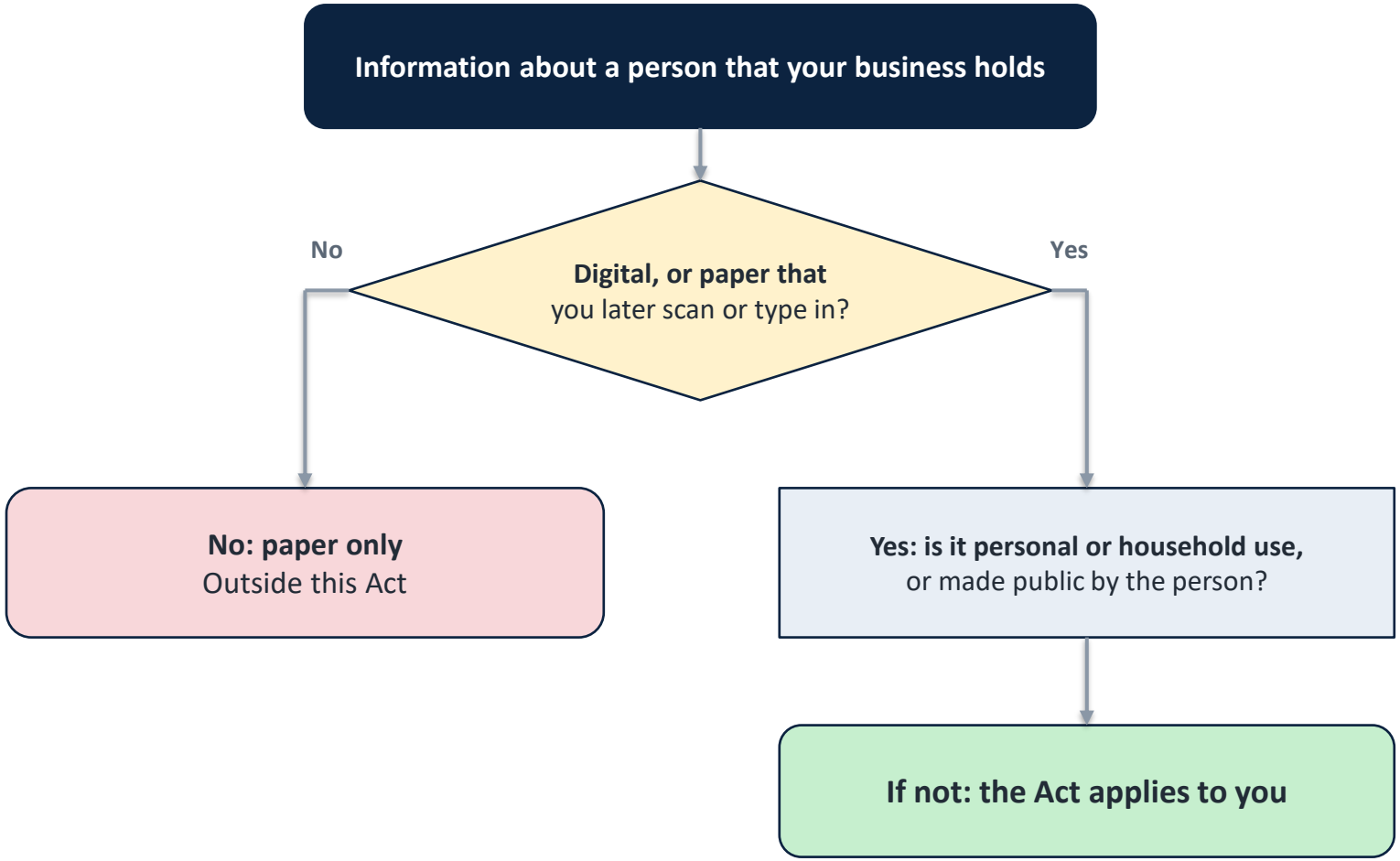


MYASHA EXPLAINS

"Fiduciary" is an old word for someone trusted with something that belongs to another, like a bank holding your money.

Personal data = anything that points to a person: name, phone, PAN, photo, customer ID.

Does it apply to you?





MYASHA EXPLAINS

There is no turnover limit. The Government may exempt some businesses, such as startups, from a few duties, but no such notification has been issued yet.

Section 3. It also covers businesses abroad that serve people in India.

The three dates

Date	What switches on	What it means for you
13 Nov 2025	Definitions, the Board, rule-making	Framework exists. No duties yet.
13 Nov 2026	Consent managers can register (Rule 4)	No new duty for an ordinary business.
13 May 2027	Notice, consent, security, breach, deletion, rights, penalties	The main duties apply.



MYASHA EXPLAINS

A consent manager is a registered app for giving and taking back consent to many businesses from one place. 13 November 2026 is a date for those apps, not a deadline for you.

What a business must do, in eight lines

1. **Have a reason:** consent, or a use the law allows.
2. **Tell people first:** a short, plain notice.
3. **Make “no” easy:** withdrawal as easy as giving consent.
4. **Answer for your vendors:** written contracts; you stay responsible.
5. **Keep it safe:** reasonable safeguards; logs for at least a year.
6. **Report leaks:** to people and the Board without delay; full report within 72 hours.
7. **Delete what you no longer need,** unless another law says keep it.
8. **Answer people:** a contact, and complaint replies within the time you publish (not more than 90 days).



MYASHA EXPLAINS

Each line has its own part in the website series, so you can read only what you need.

Asking for a yes: consent or legitimate use

You want to use a person's data for a purpose

Is it a legitimate use in section 7?

Yes

Yes
The data was given for this purpose; a law, court order, emergency or employment

No consent needed. Other duties still apply.

No

No
Marketing, analytics, sharing with partners

Give a notice, then ask for consent



MYASHA EXPLAINS

Consent is a clear yes for a stated purpose. A pre-ticked box is not a yes. Nor is silence. A legitimate use is one the law already allows, so you do not ask.

The notice: what to tell people

Stands on its own: no need to open the full privacy policy.

Plain language: in English or any of the 22 Eighth Schedule languages.

Item by item: name, mobile, address, not “your information”.

The specific purpose: and the service it enables.

The exits: how to withdraw consent, use rights, and complain to the Board.

Keep proof: which notice each person saw, and when they agreed.



MYASHA EXPLAINS

A notice is a short note telling people what you are taking and why. If it needs a law degree to understand, it is not doing its job.

Section 5 and Rule 3. Existing customers also get a notice, as soon as reasonably practicable.

Your staff, your vendors and your CCTV

Staff: payroll and attendance need no consent (section 7(i)), but data must still be safe, accurate and deleted when no longer needed.

Edges: staff photos in marketing or health apps are not plainly “for employment”; consider consent.

Vendors: a valid written contract with security terms; make them stop and erase when the purpose ends.

CCTV: digital footage where people can be recognised is personal data. A sign and a deletion cycle help.

Paper registers: outside the Act until scanned or typed in.



MYASHA EXPLAINS

A Data Processor handles data on your instructions. The law treats them as your hands: what they do, you answer for.

When data leaks: the first 72 hours

You become aware of a breach

↓

Without delay: tell each affected person
What happened, likely impact, what you are doing, what she can do, whom to contact

↓

Without delay: tell the Board
What happened, extent, when and where, likely impact

↓

Within 72 hours: detailed report to the Board
Causes, steps taken, how you will stop a repeat

Rule 7. The Board may allow more than 72 hours if asked in writing.



MYASHA EXPLAINS

A breach is not only a hack. A salary sheet sent to the wrong WhatsApp group is a breach. So is a lost laptop, or ransomware locking your files.

Keep it safe, then let it go

Protect the data: encryption, masking or tokens.

Control and watch access: logins, access rights, logs and review.

Carry on after a loss: backups.

Keep logs at least a year (Rules 6 and 8(3)), unless a law needs longer.

Delete when consent is withdrawn or the purpose is over; make vendors delete too. Tax and company-law records may need keeping longer.

Large platforms: e-commerce and social media (2 crore users) and gaming (50 lakh) erase after 3 years of inactivity, with 48 hours' warning.



MYASHA EXPLAINS

Encryption scrambles data so only someone with the key can read it. Masking shows only part, like XXXX-1234. Logs are your systems' diary of who opened what.

Children's data and people's rights

A child is anyone under 18. Get a parent's verifiable consent first (section 9, Rule 10).

No tracking, behavioural monitoring or targeted ads aimed at children. Some exemptions apply (Fourth Schedule).

People's rights from 13 May 2027: access, correction and erasure, grievance, nomination (sections 11–14).

Publish: how to make a request, a contact for data questions, and a complaint reply time of not more than 90 days.

Heavier duties for an SDF: a Data Protection Officer in India, yearly impact assessment and audit. Most small firms will not be one.



MYASHA EXPLAINS

Verifiable consent means the yes comes from a parent, and you check the parent is a real adult. A grievance is a complaint; 90 days is the outer limit for your reply.

The penalties

If a business fails in	Penalty up to
Reasonable security safeguards	₹250 crore
Telling the Board or people about a breach	₹200 crore
Extra duties for children's data	₹200 crore
Extra duties of a Significant Data Fiduciary	₹150 crore
Any other provision	₹50 crore

People have duties too: a false or frivolous complaint, or impersonation, can cost up to ₹10,000. Appeals against the Board go to TDSAT.



MYASHA EXPLAINS

These are ceilings, not fixed fines. The Board decides after an inquiry and a hearing, looking at how serious the failure was and what you did to limit the harm.

Seven months, one step at a time

Oct–Nov 2026: List the personal data you hold, where, and who sees it

↓

Dec–Jan: Write notices and consent screens

↓

Jan–Feb: Add security and deletion terms to vendor contracts

↓

Feb–Mar: Fix security gaps, switch on logs, one-page breach plan

↓

Mar–Apr: Publish a contact and a complaints desk

↓

Apr–May: Train staff, test the breach plan, notify customers

↓

13 May 2027: The main duties apply



MYASHA EXPLAINS

A suggested order, not a legal timetable. Larger businesses will need longer for each step.

Your first four steps this month

1. Name one person who will own data protection, even if it is the owner.

2. Make a rough list of personal data you hold: customers, staff, vendors' people, website visitors.

3. Note every outside service that touches it: cloud, payroll, accounting, marketing, WhatsApp.

4. Diary 13 May 2027, and read Part 1 of the series on our website.



MYASHA EXPLAINS

Start small. A rough list this month beats a perfect policy next year.



The full series is on our website: a main guide and four parts, with flowcharts and a word list.

Sources: Digital Personal Data Protection Act, 2023; Digital Personal Data Protection Rules, 2025 (G.S.R. 846(E), 13 November 2025); commencement notification G.S.R. 843(E). Read the official texts on the MeitY website and India Code before acting.

This presentation is general information, not legal advice, and does not create a client relationship. Myasha is an illustrated explainer, not a person giving advice.

Mukul Nimrani & Co., Practising Company Secretaries, Lucknow | mukulnimrani.com