FREE GUIDE · DPDP ACT, 2023 AND DPDP RULES, 2025

DPDP Readiness Starter

What is in force, what is coming, and your first 16 checks

For Indian founders, small businesses and teams that collect customer or staff details. Every point names the section of the Digital Personal Data Protection Act, 2023 (“the Act”) or the rule of the DPDP Rules, 2025 (“the Rules”) it comes from, so you can check it yourself.

Two terms you will see. Your business is a **Data Fiduciary** when it decides why and how personal data is used. The person the data is about, such as a customer or employee, is the **Data Principal**.

01 / WHERE DPDP STANDS TODAY

The law is arriving in three stages. Most day-to-day duties for businesses start on **13 May 2027**, so the next six months are your preparation window.

Stage	Date	What starts	Status on 16 Nov 2026
1	**13 Nov 2025**	Definitions; the Data Protection Board of India and how it works	In force
2	**13 Nov 2026**	Registration and duties of Consent Managers (s. 6(9); r. 4)	In force
3	**13 May 2027**	Notices, consent, security, breach reporting, children’s data, user rights, retention, cross-border rules, Significant Data Fiduciary duties and penalties	**Coming**

Source: commencement notification G.S.R. 843(E) and Rule 1 of the Rules (G.S.R. 846(E)). Stages 2 and 3 are counted from the Gazette publication of the Rules in November 2025.

ALREADY IN FORCE, OUTSIDE DPDP

• Cyber incidents must be reported to CERT-In within **6 hours** of noticing them (CERT-In Directions under s. 70B(6) of the IT Act, 28 April 2022).

• Until 13 May 2027, the IT Act’s existing data-security duty (s. 43A) and the SPDI Rules continue to apply. The Act removes them from that date (s. 44(2)).

ABOUT PENALTIES

The ₹250 crore you may have seen is a **maximum**, not a fixed fine, and no DPDP penalty can be imposed before 13 May 2027. The highest ceiling, ₹250 crore, is for failing to take reasonable security safeguards. Up to ₹200 crore applies to breach-reporting and children’s-data duties, and up to ₹50 crore to most other breaches. The Board can impose a penalty only after an inquiry finds a significant breach, weighing factors such as how serious and repeated it was and what you did to limit the harm. The evidence these checks ask you to keep is your best protection.

Act: s. 33 and the Schedule

Independent guide by TaxMedha (INTIME IT Services Pvt. Ltd.). Not legal advice. Not endorsed by the Government of India, MeitY or the DPB.

02 / YOUR FIRST 16 CHECKS

Start with checks 01 to 03 this week: everything else depends on knowing what data you hold. Tick a box only when you can show the evidence listed under it.

KNOW YOUR DATA

01 **List every place personal data comes in** ☐

Website forms, WhatsApp chats, payment links, apps, HR files and scanned paper records all count.

Evidence to keep: a one-page data list showing source, data collected and where it is stored.
Act: ss. 2(t), 3

02 **Give each use a lawful ground** ☐

Each use rests on consent or on a specific “legitimate use” in the Act. Delivering an order the customer placed is a legitimate use. Sending that customer promotions is not.

Evidence to keep: a purpose and ground column in your data list.
Act: ss. 4, 7

03 **List your vendors and check the contracts** ☐

Cloud hosting, email, payments, couriers and AI tools often handle your customers’ data. You stay responsible for what they do with it.

Evidence to keep: a vendor list with the data each receives and a note of the security terms in each contract.
Act: s. 8(1)–(2); Rules: r. 6

NOTICE AND CONSENT

04 **Write a standalone privacy notice** ☐

Plain language: what data, why, how to withdraw consent and how to complain to the Board. Keep it separate from your terms. It can be in English or any language in the Eighth Schedule.

Evidence to keep: a dated, versioned notice.
Act: s. 5; Rules: r. 3

05 **Ask for consent clearly** ☐

Use unticked boxes and ask for marketing consent separately from consent the service needs.

Evidence to keep: screenshots of each consent screen or message.
Act: s. 6(1)

06 **Make withdrawal as easy as consent** ☐

A one-click unsubscribe, or replying STOP on WhatsApp, should be enough.

Evidence to keep: a test showing a withdrawal stops the messages.
Act: s. 6(4)

07 **Record every consent** ☐

Note when consent was given, through which channel and against which notice version. Your business has to be able to prove it.

Evidence to keep: a consent log you can search.
Act: s. 6(10)

SECURITY AND INCIDENTS

08 **Put basic safeguards in place** ☐

Limit who can open customer data, use encryption or masking where you can, keep access logs and take backups.

Evidence to keep: an access list, a log setting and a restored backup test.
Act: s. 8(5); Rules: r. 6

Independent guide by TaxMedha (INTIME IT Services Pvt. Ltd.). Not legal advice. Not endorsed by the Government of India, MeitY or the DPB.

09 **Keep logs for at least one year**

The Rules require personal data, traffic data and logs from processing to be kept for at least a year.

Evidence to keep: your log retention setting.
Rules: r. 8(3)

10 **Write a one-page breach plan**

Name who decides, draft the message to affected people, and plan to inform the Board without delay, with a detailed report within 72 hours. CERT-In's 6-hour reporting already applies.

Evidence to keep: the signed plan and a practice run.
Act: s. 8(6); Rules: r. 7

RIGHTS, COMPLAINTS AND RETENTION

11 **Publish a privacy contact**

Put it on your website, app or WhatsApp business profile.

Evidence to keep: a screenshot of the published contact.
Act: s. 8(9); Rules: r. 9

12 **Set up a complaints route**

Publish how long you take to respond. The Rules cap that period at 90 days.

Evidence to keep: a complaints register.
Act: s. 13; Rules: r. 14(3)

13 **Plan for rights requests**

People can ask to access, correct or erase their data, and can nominate someone to act for them.

Evidence to keep: a short request procedure with an owner.
Act: ss. 11–14

14 **Set retention periods**

Delete data once its purpose is served, while keeping what tax and company law require you to keep.

Evidence to keep: a retention schedule for each type of data.
Act: s. 8(7); Rules: r. 8

CHILDREN AND THE WATCH LIST

15 **Check whether children use your product**

Anyone under 18 is a child. Processing their data needs verifiable consent from a parent, with similar rules for persons with disability who have a lawful guardian. Do not track, behaviourally monitor or target ads at children.

Evidence to keep: an age check and a parental-consent flow, or a note that your product is not for under-18s.
Act: s. 9; Rules: rr. 10–12

16 **Watch for new notifications**

As of this edition's check date, no business had been notified as a Significant Data Fiduciary, no startup exemption had been notified and no country had been restricted for data transfers.

Evidence to keep: a monthly check of the eGazette and MeitY.
Act: ss. 10, 16, 17

Independent guide by TaxMedha (INTIME IT Services Pvt. Ltd.). Not legal advice. Not endorsed by the Government of India, MeitY or the DPB.

When the 16 checks are done, the real work starts

This starter tells you **what** to check. Turning each check into finished work needs templates, a tracker and someone keeping the legal references up to date. That is what the paid toolkit is for.

03 / FREE STARTER AND PAID TOOLKIT

	Free starter	DPDP Implementation Toolkit
Commencement dates	Three-stage table	Dated calendar (.xlsx and .ics) with event-triggered deadlines explained
Legal references	Section and rule numbers	Claim register: each point with its ID, status, official link and date checked; applicability worksheet and gap register
Templates	What each check needs	Editable notice and consent wording, rights and grievance tracker, retention and deletion schedule
Vendors	Check the contracts	Vendor review checklist and points to cover in data-processing terms
Breaches	One-page plan outline	Breach response playbook with message drafts and a 72-hour timeline
Worked examples	—	A retailer taking WhatsApp orders and an AI product that accepts document uploads
Updates	This edition only	Dated updates for 12 months when an official change affects a claim

FREE
DPDP Implementor
A free assistant that asks about your business and gives a preliminary readiness summary and your first three fixes.
[link]

TOOLKIT
₹599 incl. GST
Handbook, editable templates, rulebook, calendar and 12 months of updates.
taxmedha.com/dpdp-toolkit

HANDS-ON HELP
Implementation support
Our team can help map your data, fill in the templates and set up controls. Quoted first. Not legal advice.
taxmedha.com

READ THE OFFICIAL TEXT

Digital Personal Data Protection Act, 2023 (MeitY): https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf

Digital Personal Data Protection Rules, 2025, G.S.R. 846(E) (MeitY copy of the Gazette): https://www.meity.gov.in/static/uploads/2025/11/53450e6e5dc0bfa85ebd78686cadad39.pdf

Commencement notification G.S.R. 843(E) and later notifications (eGazette of India): https://egazette.gov.in

CERT-In Directions of 28 April 2022 (CERT-In): https://www.cert-in.org.in

DISCLAIMER

This free guide is independently published by TaxMedha, a brand of INTIME IT Services Pvt. Ltd., for general information, education and implementation planning. It is not legal advice, a formal audit or a certification, and following it does not guarantee compliance. It is not issued, authorised or endorsed by the Government of India, MeitY, the Data Protection Board of India or any regulator. Whether a rule applies depends on your facts and the law in force. Dates for stages 2 and 3 are counted from the Gazette publication of the Rules. Check material decisions against the official text and consult a qualified Indian advocate where appropriate. Edition 1.0 · Sources checked 16 November 2026 (IST).