GNU GROUP · FIELD MANUALS

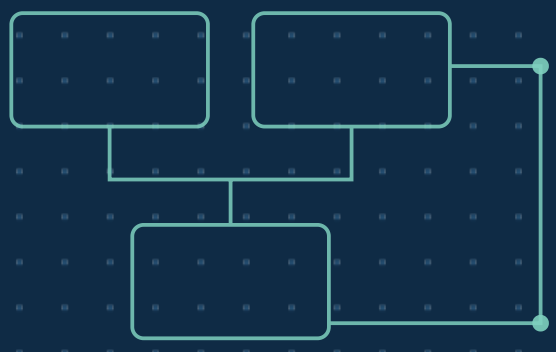
DPDP in Practice

Implementing India's Data Protection Law

A Field Manual for Every Team: Business, Legal, IT and Operations

What the Digital Personal Data Protection Act, 2023 and Rules, 2025 require, and how to put them into practice: notices and consent, people's rights, retention, security and breach response. With ready-to-adapt forms and letters, and playbooks for healthcare, IT services and financial services.

Act + Rules explained | 25 forms & drafts | Healthcare · IT services · Finance



GNU Group
gnugroup.org

Law as at 7 November 2026
Version 1.2

Who this book is for

Everyone who has a part in making an organisation comply with India's Digital Personal Data Protection Act, 2023 and Rules, 2025: founders and business heads, compliance officers and DPOs, lawyers, HR and customer-service leads, product managers, and the engineering, security and IT teams who build and run the systems. It does not assume legal training, and the technical sections are marked so that non-technical readers can skip them.

Every chapter shows the law applied to three fictional organisations: an online retailer, a hospital, and a trust that runs a school and a college. Whatever your organisation, one of them will look familiar.

How to read it

If you are...	Start with
A founder, business head or manager	Chapter 1 (the law in brief), Chapter 2 (what to build and who owns it), your sector chapter in Part II, and the readiness scorecard in 15.5.
A DPO, compliance officer or lawyer	Chapters 1, 4–7, 9–11, the obligation index (Appendix A), and the forms in Chapter 16.
HR, customer service or operations	Chapter 6 (requests and grievances), Chapter 9 (breaches), and the letters and forms in Chapter 16.
An engineer, architect or security lead	The whole book. Code listings, marked with a file name such as `sql/01_inventory.sql` , are for you; the same files are in the companion download.

How the book is organised

Start here gives five actions for the first month and a minimum path for small organisations.

Part I (Chapters 1–11) applies to every organisation. Each chapter takes one group of obligations, states what the law requires with its source, and turns it into processes, system requirements and checklists.

Part II (Chapters 12–14) contains sector playbooks for healthcare, IT services and SaaS, and banking, insurance and fintech: who is who, the other laws that apply alongside DPDP, sector exemptions, controls and a checklist.

Part III is the toolkit. Chapter 15 has templates, a breach runbook, an impact assessment outline and a readiness scorecard. Chapter 16 has 25 filled sample drafts and forms: notices, consent and withdrawal forms, request and reply letters, parental and guardian consent, a processing agreement, Board breach reports and registers. Editable Word and Excel versions are in the template pack; "Companion downloads" says how to get it and the code, and how to test the code. The appendices index every obligation by provision, set out the timeline, define terms and list sources.

Conventions

THE LAW	What the Act or the Rules require, with the provision.	BUILD	A design or control that implements it.
TRAP	A common mistake that leaves a system non-compliant.	NOTE	Context, interpretation or a point to confirm with your lawyers.
IN PRACTICE	The chapter applied to the three fictional organisations.	PROVE IT WORKS	A test that shows a control works, with owner, evidence and the usual failure.

Code listings carry a label: **Reference implementation** (tested design to adapt), **Demonstration** (a technique or first-pass check, not a control on its own) or **Production requirements outstanding** (the pattern is right but production needs more, as the listing says).

"s. 8(7)(a)" means section 8, sub-section (7), clause (a) of the Act. "r. 7(2)(b)" means rule 7, sub-rule (2), clause (b) of the Rules. "Board" means the Data Protection Board of India.

Sectors in this version

Version 1.2 has full playbooks for healthcare, IT services and SaaS, and banking, insurance and fintech; retail and education are covered through the running examples in every chapter. Full playbooks for e-commerce and consumer apps, education and edtech, HR and employment, and manufacturing and IoT are planned for a later version; until then, Part I applies to them in full.

Contents

Start here 4

PART I · FOUNDATIONS

1 The DPDP Act in brief 7
2 From obligations to architecture 12
3 Finding and inventorying personal data 16
4 Notice and consent 23
5 Legitimate uses and exemptions 30
6 Data Principal rights and grievances 34
7 Retention and erasure 40
8 Reasonable security safeguards 46
9 Personal data breach response 51
10 Processors, transfers abroad and Significant Data Fiduciaries 55
11 Children and persons with disability 60

PART II · SECTOR PLAYBOOKS

12 Healthcare: hospitals, clinics, labs and health tech 67
13 IT services, SaaS and global capability centres 72
14 Banking, insurance and fintech 77

PART III · TOOLKIT AND REFERENCE

15 Toolkit: templates and checklists 84
16 Sample drafts and forms 89
Companion downloads 108
A Obligation index 110
B Timeline 112
C Glossary 113
D Sources 115
Version history 118
Licence: GNU-IND-1.0 and the DPDP in Practice addendum 119

START HERE

Start here

Five things to do in the next month, whatever your size, and a minimum path for small organisations that do not have an engineering team to spare. Most duties apply from 13 May 2027.

Five actions for this month

#	Action	Who	What you will have at the end	See
1	**Name one accountable owner** and a contact person who answers people's questions about their data.	CEO or board	A one-line appointment and a published contact (s. 8(9); r. 9). An owner for each of the components in Chapter 2.	Ch. 2
2	**List every system and vendor that holds personal data**, including spreadsheets, chat groups and software paid for by card.	Owner with each department head	A first record of processing, even if rough.	Ch. 3; T24
3	**Record why you process each kind of data:** consent, or which clause of s. 7.	Owner with legal	A ground and a reason against every purpose; a list of purposes that need consent you do not yet have.	Ch. 4–5; T22
4	**Inspect every place you collect data**: website and app forms, paper forms, call scripts, registers at the front desk.	Product, operations	A list of collection points with or without a notice, and bundled consents to split.	Ch. 4; T01–T03
5	**Set up an incident contact** and a way for staff and vendors to report a suspected breach within hours.	IT or security lead	A named incident commander, a phone and e-mail that are watched, and the CERT-In and Board steps written down.	Ch. 9; T17

Then use the readiness scorecard (15.5) to plan the rest, critical items first.

The minimum path for a small organisation

A clinic, a coaching centre, a school or a small online shop can meet most duties with registers, the settings of the software it already uses, and its vendors' processes. The code in this book is for organisations whose volumes need automation; you can leave it for later.

Duty	The small-organisation way	Evidence to keep
Know your data	Fill in the processing register in the Excel workbook; review it every quarter.	The register, with review dates
Notice and consent	One plain notice on your website (T01); the same items on paper and online forms; separate unticked boxes for optional uses, using your form tool's own checkbox and timestamp.	Copies of each notice version; the form tool's export of who agreed, when, to which version
Withdrawal	A link or reply keyword that unsubscribes, plus a form (T06); a weekly check that the mailing tool has applied it.	Withdrawal confirmations
Requests and grievances	A shared mailbox and the requests sheet in the workbook; letters T08–T11.	The requests sheet with due dates and outcomes
Retention and erasure	The retention sheet; a calendar reminder each month to delete what is due; ask vendors to delete and confirm.	Deletion log; vendor confirmations
Security	Multi-factor sign-in on e-mail and every cloud tool; one account per person; admin rights for few; automatic backups; laptop encryption; screen locks.	Screenshots of settings; backup restore test
Breaches	T17 printed and pinned; phone list; templates T18–T21 ready.	A short drill once a year

Duty	The small-organisation way	Evidence to keep
Vendors	Send T16 and attach the T15 schedule at renewal; keep the processor sheet.	Signed schedules; questionnaire answers

IN PRACTICE: THE MINIMUM PATH AT NAVADEEP

Navadeep Education Trus

With a three-person IT team, the trust spends its first month on the five actions: the trust secretary is named owner and the school office e-mail is published as the contact; the register lists 23 systems, 6 of them unknown to IT; admission forms are found to bundle photo consent into admission; the bus contractor's GPS app is found to have no contract terms on data. Everything else waits until those are fixed.

The first 90 days

When	Do	Done when
Month 1	The five actions above. Agree the owner of each component in Chapter 2.	Owner named; first register; incident contact live
Month 2	Fix the collection points: notices (T01), separate optional consents (T02), withdrawal route (T06). Send the processing schedule (T15) and questionnaire (T16) to your main vendors.	No bundled consents left; main vendors have the schedule
Month 3	Set up requests and grievances (T07–T11), the retention schedule (T25) and the breach templates (T17–T21). Run a one-hour breach drill.	A test request answered on time; drill timings recorded
Then	Score yourself on the readiness scorecard (15.5) and fix every critical gap before 13 May 2027.	No critical item below 2

Where to find the downloads

The editable forms, the Excel registers and the tested code are in the companion downloads. The page "Companion downloads" before the appendices lists every file, the versions they were tested with and the results you should see.

CHAPTER 1

The DPDP Act in brief

What the law covers, who carries which duty, when each part starts, and what a failure costs. Everything later in the book builds on the vocabulary set out here.

IN BRIEF

- The Act applies to **digital** personal data processed in India, and to processing abroad that serves people in India (s. 3).
- Personal data may be processed only with **consent** or for one of the **legitimate uses** listed in section 7 (s. 4). There is no general "legitimate interests" ground.
- The organisation that decides why and how data is processed (the **Data Fiduciary**) stays responsible for everything its vendors do (s. 8(1)).
- Most duties start on **13 May 2027**. Consent Manager registration starts on **13 November 2026**.
- Penalties are imposed per breach and go up to **₹250 crore** for failing to take reasonable security safeguards (Schedule to the Act).

1.1 Why this law needs every team

Most of the Digital Personal Data Protection Act, 2023 ("the Act") and the Digital Personal Data Protection Rules, 2025 ("the Rules") cannot be satisfied by a policy document. A notice has to be shown at the right moment in a sign-up flow. Consent has to be recorded in a way that can be proved later, because the Act places that burden on the organisation (s. 6(10)). Erasure has to reach backups and vendors. Logs have to exist, be kept for a year and then be deleted (r. 6(1)(e), r. 8(3)). A breach report with six specific elements has to reach the Data Protection Board within 72 hours (r. 7(2)(b)).

Each of these is a system requirement. Lawyers decide what the law means for your organisation; business owners decide which purposes the organisation pursues; engineers and operations teams decide whether it can actually do what it promises. This book is written so that all of them can work from the same page.

Three organisations you will meet in every chapter

The law reads the same for a grocery app, a hospital and a school, but the work looks different in each. Every chapter therefore ends its explanation with an "In practice" box showing how three fictional organisations apply it. They are invented, and so are all their names, figures and systems; any resemblance to a real organisation is unintended.

	Business Nilaya Retail Pvt. Ltd.	Hospital Aranya Hospital	Education Navadeep Education Trust
What it does	Online grocery app and website in Bengaluru, with a marketplace for local sellers	300-bed multispeciality hospital in Pune: outpatients, inpatients, lab, pharmacy, radiology, paediatrics, a psychiatry unit, teleconsultation and a patient app	Runs Navadeep Public School (nursery to Class 12) and Navadeep College (engineering and commerce, with hostels) in Nashik
Whose data	About 20 lakh customers, 6,000 sellers, 400 staff and delivery partners	About 1,200 outpatients a day, inpatients, 1,100 staff, visitors	2,400 schoolchildren and their parents; 3,000 college students, a few aged 17 when they join; 450 staff; alumni; applicants
Most sensitive data	Sellers' PAN images, payment details, purchase history	Diagnoses, test results, mental health records, children's records	Children's records and location on school buses, marks, health check-up results, hostel CCTV
Key vendors	Delivery partners, payment aggregator, cloud hosting, messaging, a US help-desk tool	Hospital information system (HIS) vendor, reference lab, PACS, insurers and TPAs, ABDM	School ERP, a learning app, bus GPS contractor, e-mail and office suite, recruiters through the placement cell

	Business Nilaya Retail Pvt. Ltd.	Hospital Aranya Hospital	Education Navadeep Education Trust
Starting point, November 2026	Consent bundled into sign-up; no request process; vendor contracts silent on data	Shared ward logins; patient lists in staff chat groups; no breach procedure	Admission forms with blanket consent; photos on the website; class marks shared in parent groups

NOT LEGAL ADVICE

This book explains the Act and Rules as they stood on 7 November 2026 and shows how to build systems that meet them. It is not legal advice. Where a decision depends on how a provision applies to your organisation (whether a use counts as a legitimate use, how long a sector law requires you to keep a record), take it with your legal team and record the reasoning.

1.2 What the Act covers

Section 3 sets the scope in three parts.

Situation	Covered?	Provision
Personal data collected in digital form and processed in India	Yes	s. 3(a)(i)
Personal data collected on paper and digitised later, processed in India	Yes, once digitised. Paper-only records are outside the Act.	s. 3(a)(ii)
Processing outside India connected with offering goods or services to people in India	Yes	s. 3(b)
An individual's personal or domestic use	No	s. 3(c)(i)
Data the person made public herself, or that someone was legally required to publish	No	s. 3(c)(ii)

"Personal data" means any data about an individual who is identifiable by or in relation to that data (s. 2(t)). "Processing" covers almost anything a system does with it: collection, recording, storage, retrieval, use, combination, indexing, sharing, restriction, erasure (s. 2(x)). For an engineer the practical reading is simple: if a table, file, log line, event or model input can be tied to a person, it is in scope.

THERE IS NO "SENSITIVE" CATEGORY

Unlike the IT Act's SPDI Rules of 2011 and unlike the GDPR, the DPDP Act does not define a special category of sensitive personal data. Health, financial and biometric data get no separate legal regime under the Act itself. That does not lower the bar: the security duty is "reasonable" safeguards (s. 8(5)), and what is reasonable for medical records is not what is reasonable for a newsletter list. Sector laws (Part II) also add their own rules.

1.3 The actors

The Act names five roles. The same company can hold several of them at once, for different data.

Role	Who it is	Engineering consequence
Data Principal	The individual the data is about. For a child (under 18, s. 2(f)) it includes the parents or lawful guardian; for a person with disability who has a lawful guardian, it includes the guardian (s. 2(j)).	Every record needs a link to the person it belongs to, or rights requests cannot be answered.

CHAPTER 9

Personal data breach response

Every personal data breach must be reported to the Board and to each affected person, whatever its size. The clocks are short and run in parallel with CERT-In's. A breach programme is a pipeline, rehearsed before it is needed.

IN BRIEF

- A personal data breach includes unauthorised processing, accidental disclosure, and loss of access or availability, not only theft (s. 2(u)).
- On becoming aware: tell each affected person without delay (r. 7(1)); tell the Board without delay, then send a detailed report within 72 hours (r. 7(2)).
- There is no threshold. The Act does not exempt small or low-risk breaches from notification.
- CERT-In's 6-hour reporting, and sector regulators' own reporting, run alongside.
- Failing to notify can cost up to ₹200 crore, on top of any penalty for the security failure itself.

9.1 What counts as a breach

THE LAW

"Personal data breach" means any unauthorised processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data, that compromises its confidentiality, integrity or availability (s. 2(u)). In the event of a personal data breach, the Data Fiduciary must give the Board and each affected Data Principal intimation of it in the prescribed form and manner (s. 8(6)).

The definition is wide. Examples that qualify, though teams often do not treat them as breaches:

- An e-mail with a customer spreadsheet sent to the wrong recipient (accidental disclosure).
- An employee looking up a celebrity's records without a work reason (unauthorised processing).
- Ransomware that encrypts a patient database, even if nothing was copied (loss of access; availability).
- A storage bucket left public, even if logs show no download yet (likely unauthorised access; investigate).
- A bug that shows one customer another customer's order (disclosure).
- A processor's incident affecting your data (your obligation, because the processing is on your behalf: s. 8(1), (5)).

NO MATERIALITY THRESHOLD

Many regimes only require notification when a breach is likely to cause harm. Section 8(6) and rule 7 contain no such threshold: every personal data breach is notified to the Board and to each affected person. The severity shapes the content of the notice and the response, not whether notice is given. Build the pipeline to handle many small notifications, not just the rare large one.

9.2 The clocks

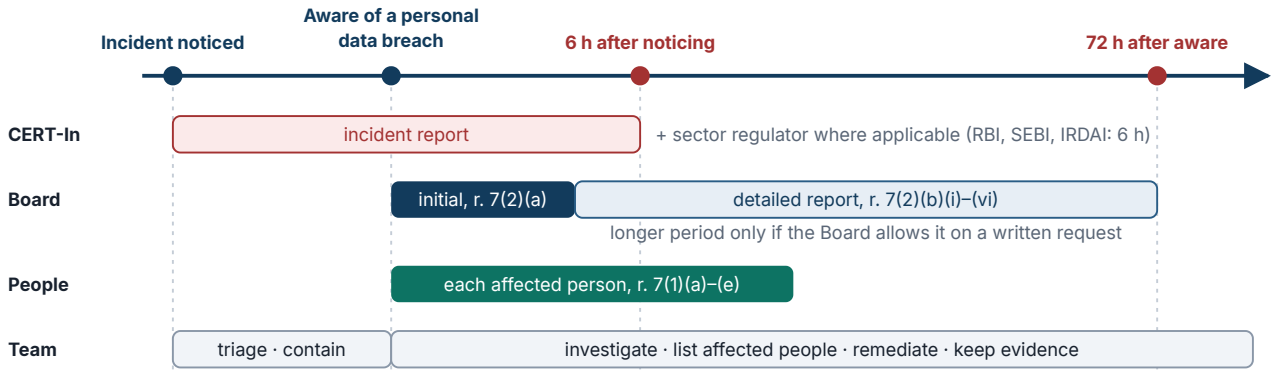


Figure 9.1 The parallel reporting clocks. CERT-In counts from noticing the incident; the DPDP clocks from becoming aware of a personal data breach. Sector regulators may add their own, often 6 hours.

To whom	When	What	Source
Each affected Data Principal	Without delay, to the best of your knowledge	Concise, clear, plain notice through her user account or a registered contact mode, with: (a) a description of the breach, including its nature, extent and the timing of its occurrence; (b) the likely consequences for her; (c) mitigation measures taken or under way; (d) safety measures she can take; (e) business contact of a person who can answer her questions.	r. 7(1)
Board: initial	Without delay	Description of the breach: nature, extent, timing and location of occurrence, likely impact.	r. 7(2)(a)
Board: detailed report	Within 72 hours of becoming aware, or a longer period the Board allows on a written request	(i) updated, detailed description; (ii) broad facts on events, circumstances and reasons; (iii) mitigation measures implemented or proposed; (iv) any findings about the person who caused it; (v) remedial measures to prevent recurrence; (vi) a report on the intimations given to Data Principals.	r. 7(2)(b)
CERT-In	Within 6 hours of noticing	Incident report in CERT-In's format, for the incident types in its directions, which include data breaches and leaks.	CERT-In directions, 2022
Sector regulator	As its directions require	For example RBI (through its DAKSH platform), SEBI and IRDAI each require reporting within 6 hours (Chapter 14).	Sector rules

"BECOMING AWARE"

Rule 7 runs from becoming aware of a personal data breach. Define in your runbook when that is: for example, when the incident commander, on the facts available, judges it more likely than not that personal data has been compromised. Record the time and the reasoning. Starting the clock late is hard to defend when your own logs show the alert arrived earlier.

9.3 The pipeline

1. **Detect.** Alerts from monitoring (Chapter 8), processors, employees, customers, researchers and the press all land in one queue with a timestamp.
2. **Triage (first hour).** Incident commander assigned. Is personal data involved? Which systems and data elements (from the inventory)? How many people? Is it ongoing?
3. **Contain.** Revoke credentials, close exposure, isolate systems, preserve evidence. Containment comes before perfect knowledge.

Purpose	Likely ground	Notes
Notifiable disease reporting, medico-legal cases, court orders	s. 7(d), (e)	Disclosure that a law requires to the State or its authorities (s. 7(d)), or that a court orders (s. 7(e)). Section 7(c) is for functions of the State itself, not for a private hospital.
Staff data: rosters, credentials, payroll	s. 7(i)	Employment purposes (Chapter 5).
Marketing health check packages, follow-up campaigns	Consent	Separate, unbundled consent; easy withdrawal (Chapter 4).
Research and registries	Consent, or s. 17(2)(b) with r. 16	The Act does not apply to processing necessary for research, archiving or statistics where data is not used for decisions specific to a person and the Second Schedule standards are followed. Ethics committee approval and clinical trial rules apply separately.

12.3 Emergency access

Section 7(f) lets a clinician who is not on a patient's care team see the record in an emergency. Without controls the same feature is the most common route to snooping on records of celebrities, colleagues and relatives, which is unauthorised processing and so a personal data breach (s. 2(u)). Build break-glass access with four properties: a stated ground and reason, a short time limit, a log of every read, and review by someone else.

`sql/10_emergency_access.sql` REFERENCE IMPLEMENTATION

```
-- Break-glass access to patient records for medical emergencies (PostgreSQL 16).
-- Ground: s. 7(f) medical emergency, s. 7(g) epidemic or public-health measures.
CREATE SCHEMA IF NOT EXISTS clinical;
SET search_path = clinical;

-- Normal access: the clinician is on the patient's care team for this episode.
CREATE TABLE care_team (
  patient_id text NOT NULL,
  actor      text NOT NULL,
  from_ts    timestamptz NOT NULL DEFAULT now(),
  to_ts      timestamptz,
  PRIMARY KEY (patient_id, actor, from_ts)
);

CREATE TYPE emergency_ground AS ENUM
  ('s7f_threat_to_life', 's7f_immediate_threat_to_health', 's7g_public_health');

CREATE TABLE emergency_access (
  access_id     bigint GENERATED ALWAYS AS IDENTITY PRIMARY KEY,
  patient_id    text NOT NULL,
  actor         text NOT NULL,
  ground        emergency_ground NOT NULL,
  justification text NOT NULL CHECK (length(justification) >= 20),
  started_at    timestamptz NOT NULL DEFAULT now(),
  ends_at       timestamptz NOT NULL DEFAULT now() + interval '4 hours',
  reviewed_by   text,
  reviewed_at   timestamptz,
  outcome       text CHECK (outcome IN ('justified', 'not_justified')),
  CHECK (ends_at > started_at AND ends_at <= started_at + interval '24 hours'),
  CHECK (reviewed_by IS NULL OR reviewed_by <> actor),          -- no self-review
  CHECK ((reviewed_by IS NULL) = (outcome IS NULL))
);

-- Every read decision is logged, allowed or not (r. 6(1)(c)).
CREATE TABLE access_log (
  at         timestamptz NOT NULL DEFAULT now(),
  actor      text NOT NULL,
  patient_id text NOT NULL,
  allowed    boolean NOT NULL,
  basis      text NOT NULL
);

CREATE FUNCTION can_read(p_actor text, p_patient text) RETURNS boolean
```

15.5 Readiness scorecard

For each line, first decide whether it applies to you. Then score it 0 (not started), 1 (partly in place) or 2 (in place with evidence), name an owner, link the evidence, and set a date for anything below 2. The same scorecard, with formulas, is a sheet in the Excel workbook.

A HIGH TOTAL CAN HIDE A MISSING CONTROL

You are **not ready** while any applicable critical line scores below 2, whatever the total. A score of 24 out of 26 with no working breach route is not readiness.

Area	Critical?	In place when	Ch.	Score	Owner and evidence link	Fix by
Inventory	Yes	Every system, purpose, ground, element, processor and country recorded; gap report reviewed monthly.	3			
Notice and consent	Yes	Versioned notices from the inventory; separate optional consents; ledger or form-tool records; withdrawal propagates and is confirmed.	4			
Legacy consent	If you hold pre-2027 consents	Section 5(2) notices sent to existing users, with delivery records.	4			
Legitimate uses	Yes	Each non-consent ground explained and approved (T22).	5			
Rights	Yes	Published means and identifiers; requests tracked with due dates; access replies include sharing lists.	6			
Grievances	Yes	One published response period, not over 90 days; at-risk report.	6			
Retention and erasure	Yes	Rules with legal basis; legal holds; erasure with evidence; one-year logs; Third Schedule clock if applicable.	7			
Security	Yes	Each r. 6(1) item mapped to controls with evidence; CERT-In logs and clock sync.	8			
Breach response	Yes	Runbook, templates, notification route, register with clocks; drill in last 12 months.	9			
Processors and transfers	Yes	Processors under contract with clause flags; transfer check clean.	10			
Children and guardians	If you process children's or guardians' data	Status and basis per person; verified parents and guardians; exemptions per purpose.	11			
Sector rules	If your sector has them	Sector retention, localisation and reporting duties loaded and tested.	12–14			
Governance	No	Owners for each component; contact person or DPO published; training done.	2			

No.	Form or draft	Basis
T23	Data Protection Impact Assessment (filled summary)	s. 10(2)(c); r. 13(1)–(3)
T24	Record of processing (register)	s. 8(4); supports s. 5, 8(7), 11; r. 3
T25	Retention schedule	s. 8(7), 8(8), 12(3); r. 8; Third Schedule

16.1 Notices and consent

What people see before and when you collect their data.

T01 Privacy notice (website and app)

Use: Publish on the website and in the app; link it from every consent request. Generate the data table from your inventory so it stays accurate.
Basis: s. 5, 6, 8(9), 11–14; r. 3, 9, 14(1), 14(3)

How Nilaya uses your personal data

Version 3, effective [date]. Read this in English, Hindi, Kannada, Tamil or Marathi at nilaya.example/privacy. Other languages listed in the Eighth Schedule to the Constitution are available on request.

1. Who we are

Nilaya Retail Pvt. Ltd. ("Nilaya", "we") runs the Nilaya grocery delivery app and website. We decide why and how your personal data is used, so we are the Data Fiduciary for it under the Digital Personal Data Protection Act, 2023.

2. What we collect and why

Personal data	Purpose	What it enables for you	Basis
Name, mobile number	Create and secure your account	Sign-in with one-time password	Your consent
Delivery address, delivery instructions	Deliver your orders	Doorstep delivery	Your consent
Order history, payment status	Process orders, refunds and invoices	Orders, returns, GST invoices	Your consent
Card or UPI details	Take payment (handled by our payment provider; we do not store card numbers)	Paying for orders	Your consent
Precise location, only while you use the app	Show stores and slots near you	Faster, accurate delivery slots	Your consent (optional)
Order history	Send offers you may like by SMS or WhatsApp	Personalised offers	Your consent (optional)
Messages to customer support	Answer your questions and complaints	Support	Data you give us for that purpose (s. 7(a))

You can use Nilaya without the optional items. We do not collect data about children for marketing, and we do not sell personal data.

3. Who we share it with

- Delivery partners, to deliver your order (name, mobile number, address, delivery instructions).
- Our payment provider and your bank, to take payment and process refunds.
- Cloud hosting, messaging and customer-support service providers who work for us under contracts that require them to protect your data and use it only on our instructions.
- Government authorities, courts or regulators where a law or order requires it.

You can ask us for the names of the organisations we have shared your data with (section 6 below).

#	Question	Answer / evidence
12	Do you report incidents to CERT-In within 6 hours and keep ICT logs for 180 days in India?	

Completed by (name, role)	
Date	
Reviewed by us; decision	☐ Approve ☐ Approve with conditions ☐ Reject

16.5 Personal data breaches

Internal record, Board intimations and the notice to people, filled in for one example incident.

T17 Incident report and breach decision log

Use: Opened by the incident commander for every incident; the decision log records when the organisation became aware of a personal data breach.
Basis: s. 2(u), 8(6); r. 6(1)(c), 7

Incident ID	PDB-2027-014
Detected	14 Aug 2027, 09:40 IST, by cloud security alert
Summary	Storage bucket holding KYC images for seller onboarding was publicly readable
Systems	seller-kyc-store (Mumbai region)
Data elements	PAN card images, seller name, photo
People affected (estimate)	41,210 sellers
Contained	14 Aug 2027, 10:15 IST: public access removed, keys rotated
Incident commander	R. Kulkarni, Head of Security

Decision log

Time	Decision and reasoning	By
09:55	Bucket holds PAN images and has been publicly readable since 11 Aug. **Aware of a personal data breach** from this time: personal data was accidentally disclosed to anyone on the internet. No proof of download is needed for that.	R. Kulkarni, A. Shah (DPO)
10:40	Board initial intimation sent (r. 7(2)(a)).	A. Shah
11:20	Access logs show 3 downloads from unknown IP addresses on 12 Aug: data was also acquired. Impact raised; awareness time unchanged.	R. Kulkarni
11:45	CERT-In report filed (within 6 hours of 09:40).	Security
14 Aug 18:00	Notices to 41,210 sellers sent by e-mail and in-app; 312 bounced, follow up by SMS.	Comms
17 Aug 09:30	Board detailed report sent (within 72 h of 09:55 on 14 Aug).	A. Shah

HOW TO ADAPT IT

A personal data breach includes accidental disclosure (s. 2(u)), so a public bucket of personal data is a breach once you know it was exposed; do not wait for proof that someone downloaded it. Write down the reasoning when you decide you are aware: the r. 7 clocks run from that moment, and the Board will compare it with your logs.

APPENDIX A

Obligation index

Every duty of a Data Fiduciary in the Act and Rules, when it applies, and where this book covers it. Dates follow the commencement notification and rule 1; "May 2027" means 13 May 2027.

Provision	Duty	From	Ch.
s. 4	Process personal data only for a lawful purpose, with consent or for a legitimate use.	May 2027	1, 4, 5
s. 5(1); r. 3	Give a notice with or before every consent request: itemised data, purposes, how to withdraw, exercise rights and complain.	May 2027	4, 15
s. 5(2)	Give a notice, as soon as reasonably practicable, to people who consented before commencement.	May 2027	4
s. 5(3)	Offer the notice in English or any Eighth Schedule language.	May 2027	4
s. 6(1)–(3)	Consent free, specific, informed, unconditional, unambiguous, by clear affirmative action, limited to necessary data; in clear and plain language.	May 2027	4
s. 6(4)–(6)	Let people withdraw as easily as they consented; stop processing and make processors stop within a reasonable time.	May 2027	4
s. 6(7)–(9); r. 4; First Schedule	Consent may be given, managed and withdrawn through a registered Consent Manager.	13 Nov 2026 (s. 6(9), r. 4); May 2027 (rest)	4
s. 6(10)	Be able to prove notice and consent.	May 2027	4
s. 7	Use a legitimate use only within its terms; record which one.	May 2027	5
s. 7(b); r. 5; Second Schedule	State processing for subsidies, benefits and services to follow the standards.	May 2027	5
s. 8(1)	Remain responsible for processing by processors, whatever the contract says.	May 2027	10
s. 8(2)	Engage processors only under a valid contract.	May 2027	10
s. 8(3)	Ensure completeness, accuracy and consistency where data is used for decisions or disclosed to another fiduciary.	May 2027	6, 10
s. 8(4)	Implement technical and organisational measures for effective observance.	May 2027	2
s. 8(5); r. 6	Take reasonable security safeguards, at least the seven in r. 6(1).	May 2027	8
s. 8(6); r. 7	Intimate every personal data breach to the Board and each affected person.	May 2027	9
s. 8(7)	Erase on withdrawal or when the purpose is no longer served, and make processors erase, unless law requires retention.	May 2027	7
s. 8(8); r. 8(1)–(2); Third Schedule	Large e-commerce, gaming and social media platforms: erase after three years' inactivity, with 48 hours' notice.	May 2027	7
r. 8(3); Seventh Schedule	Keep personal data, traffic data and logs of processing for at least one year.	May 2027	7, 8
s. 8(9); r. 9	Publish the business contact of the DPO or a contact person, and give it in every response to a rights request.	May 2027	6
s. 8(10); r. 14(3)	Run an effective grievance mechanism and publish a response period of not more than 90 days.	May 2027	6
s. 9(1); r. 10, 11	Obtain verifiable consent of a parent or lawful guardian.	May 2027	11
s. 9(2)	No processing likely to harm a child's well-being.	May 2027	11

END OF SAMPLE

What is in the full book

DPDP in Practice: Implementing India's Data Protection Law. Version 1.2, law as at 7 November 2026.

Part	What you get
Start here	Five actions for the first month, a minimum path for small organisations, and a 90-day plan.
Part I: Foundations (Chapters 1–11)	The Act and Rules 2025 explained, every point tied to its section or rule, from inventory and consent to breaches, vendors and children. Each chapter applies the law to a retailer, a hospital and a school and college, with a "Prove it works" test and a checklist.
Part II: Sector playbooks (Chapters 12–14)	Healthcare; IT services, SaaS and GCCs; banking, insurance and fintech: who is who, the other laws that apply alongside DPDP, controls and checklists.
Part III: Toolkit and reference	Templates and a breach runbook; a readiness scorecard with a critical-gap rule; 25 filled sample drafts and forms; an obligation index, timeline, glossary, sources with official links, and a register of open interpretations.

Editions

Edition	Includes
Book (PDF or EPUB)	The complete book, about 120 pages.
Toolkit edition (PDF)	The complete book, with two files attached inside the PDF: the template pack (25 editable Word forms and an Excel workbook of registers with deadline, gap and readiness formulas) and the companion code (tested PostgreSQL and Python examples with their tests).
Team and institution licences	For companies, consultancies, training institutes and colleges.

Prices, the errata page and team licences: **gnugroup.org**.

WHO IT IS FOR

DPOs and compliance officers, IT and security leads, and the consultants who support them; founders, HR and operations heads who need to know what to do and who owns it.

GOOD TO KNOW

Not legal advice: it explains the law so that organisations can build processes and systems, and flags where to take legal advice. You may share this sample freely, unchanged. © 2026 Gnu IT Solutions & Services Pvt. Ltd. · gnugroup.org