DPDP COMPLIANCE READINESS TOOLKIT

Process, Timeline and Self-Assessment for the Digital Personal Data Protection Act, 2023

Document Title	DPDP Compliance Readiness Toolkit
Version	1.0 (October 2026)
Prepared By	Quinfy Technology Pvt. Ltd. and Quinfy Inc.
Intended Users	Compliance, HR, IT/Security, Legal and leadership teams
Classification	Public. Free to download and use within your organisation.
Review Frequency	Updated when MeitY issues material guidance

Version Control

Version	Date	Prepared By	Summary of Changes
1.0	29 Oct 2026	Quinfy	First release

Important: this toolkit is general guidance and not legal advice. Dates and rule references reflect public sources at the time of writing. Please confirm the current position with qualified legal counsel and the official MeitY notifications.

1. Purpose and how to use this toolkit

India's Digital Personal Data Protection (DPDP) Act, 2023 and the DPDP Rules, 2025 place duties on every organisation that decides why and how personal data is processed (a Data Fiduciary). This toolkit helps you answer two questions: where do we stand today, and what do we need to do before the deadlines?

Use it in this order:

- Read the government timeline in Section 2 and agree an internal target date.
- Run the 30-point self-assessment in Section 3 with the people who own each area, and total your score using the guide in Section 4.
- Use the six-phase roadmap in Section 5 to plan the work, and the responsibilities matrix in Section 6 to assign owners.
- Collect proof as you go in the evidence register (Section 7). If you hire or verify people, work through the hiring addendum in Section 8.

2. Government timeline

The DPDP Rules, 2025 were notified by the Ministry of Electronics and Information Technology (MeitY) on 13 November 2025 (G.S.R. 846(E)). They apply in three stages.

Date	Provisions that apply	What it means in practice
13 Nov 2025 (in force)	Rules 1, 2 and 17 to 21: short title, definitions and the Data Protection Board of India	The Board exists and the complaint and penalty machinery is available. Few direct operational duties for most organisations.
13 Nov 2026 (12 months)	Rule 4: registration and obligations of Consent Managers	Relevant if you plan to act as, or work with, a Consent Manager. Use this as your first internal milestone.
13 May 2027 (18 months)	Rules 3 and 5 to 16, 22 and 23: notice, consent, security safeguards, breach reporting, retention and erasure, children's data, data principal rights, Significant Data Fiduciary duties, cross-border transfers	Full compliance expected. Your processes, contracts and controls need to be working and evidenced by this date.

Watch point: public commentary notes that the final stage could be brought forward. We recommend working to an internal target of 31 March 2027 for the core controls, which leaves a buffer before 13 May 2027.

Penalties: the Act allows monetary penalties of up to INR 250 crore for failure to take reasonable security safeguards to prevent a personal data breach, with other contraventions carrying their own penalty ceilings under the Schedule to the Act.

3. Self-assessment checklist

For each question, mark Yes (fully in place and evidenced), Part. for partial (in place but incomplete or not evidenced) or No. Record the evidence you would show an auditor and the person who owns the answer.

A. Governance and accountability

#	Control question	Reference	Yes	Part.	No	Evidence / owner
1	A senior owner is named for DPDP compliance and leadership/board understands the obligations and penalty exposure.	Act s.8(1)				
2	A data inventory maps every system, vendor, file store and paper-to-digital process that holds personal data (customers, candidates, employees).	Act s.8				
3	We have assessed whether we could be notified as a Significant Data Fiduciary and, if so, planned for a Data Protection Officer in India, annual impact assessment and independent audit.	Act s.10				

#	Control question	Reference	Yes	Part.	No	Evidence / owner
4	A written, approved privacy policy and supporting procedures exist and are available to staff.	Act s.8				
5	Staff who handle personal data (HR, sales, support, IT) have been trained and training is recorded.	Act s.8(1)				

B. Notice and consent

#	Control question	Reference	Yes	Part.	No	Evidence / owner
6	Notice is given before or at collection, in plain language, itemising the data and purpose, how to exercise rights and how to complain to the Data Protection Board.	Act s.5; Rule 3				
7	Consent is free, specific, informed, unconditional and unambiguous, given by a clear affirmative action, and not bundled with unrelated terms.	Act s.6				
8	Consent records are timestamped, linked to the purpose and retrievable on request.	Act s.6				
9	Withdrawing consent is as easy as giving it, and withdrawal reaches processors.	Act s.6(4)				
10	We have identified data collected before the Act and decided how to give notice for it.	Act s.5(2)				
11	Any reliance on 'legitimate uses' (including employment purposes) is documented, limited to what is needed, and reviewed by counsel.	Act s.7				

C. Rights of data principals

#	Control question	Reference	Yes	Part.	No	Evidence / owner
12	People can ask for a summary of their personal data and the identities of those it is shared with, and we can respond within a defined time.	Act s.11				
13	We can correct, complete, update and erase data on request, including copies held by processors.	Act s.12				

#	Control question	Reference	Yes	Part.	No	Evidence / owner
14	A grievance channel is published, with a named contact and a response timeline, before people need to approach the Board.	Act s.13				
15	People can nominate another person to exercise their rights in case of death or incapacity, and we have a process for it.	Act s.14				

D. Security and breach readiness

#	Control question	Reference	Yes	Part.	No	Evidence / owner
16	Reasonable security safeguards are in place and evidenced: encryption or masking, access control, backups and continuity.	Act s.8(5); Rule 6				
17	Access to candidate and employee data follows least privilege, with logging and monitoring, and logs are retained for at least one year.	Rule 6				
18	A breach response plan names who informs the Data Protection Board and affected individuals, including a detailed report within 72 hours.	Act s.8(6); Rule 7				
19	The breach plan has been tested through a drill in the last 12 months.	Rule 7				
20	Endpoints, email and shared drives that hold personal data are covered by security controls (no uncontrolled copies in inboxes or personal devices).	Act s.8(5)				
21	Independent security assurance (for example ISO 27001 or SOC 2 Type II) is held or required of key vendors.	Act s.8(5)				

E. Processors and cross-border transfers

#	Control question	Reference	Yes	Part.	No	Evidence / owner
22	Every processor is bound by a valid contract covering instructions, security, breach alerts, sub-processors and return or deletion of data.	Act s.8(2)				

#	Control question	Reference	Yes	Part.	No	Evidence / owner
23	We keep a current register of processors and sub-processors.	Act s.8(2)				
24	Cross-border transfers are mapped and checked against any restrictions the Government notifies.	Act s.16				
25	We review processors at least annually and understand that we stay responsible for their processing.	Act s.8(1)				

F. Retention, erasure, accuracy and children

#	Control question	Reference	Yes	Part.	No	Evidence / owner
26	A retention schedule sets how long each category of data is kept and why, and data is erased once the purpose ends unless law requires retention.	Act s.8(7)				
27	Erasure is verified end to end, including at processors, and we can show it happened.	Act s.8(7)				
28	If we process data of anyone under 18, we obtain verifiable parental consent and avoid tracking or behavioural monitoring of children.	Act s.9; Rule 10				
29	Contact details of a person who can answer questions about our data processing are published.	Act s.8(9)				
30	Where data is used to make decisions about people or is shared, we take steps to keep it complete, accurate and consistent.	Act s.8(3)				

4. Scoring guide

Score Yes = 2, Partial = 1, No = 0. The maximum is 60.

Total score	Readiness level	What to do
50 to 60	On track	Close remaining gaps, collect evidence and schedule an annual review.
35 to 49	Gaps to close	Prioritise any No answers in sections B, D and E first. Aim to finish by 31 March 2027.
20 to 34	Significant work needed	Start the roadmap now with an appointed owner and a funded plan.
Below 20	Not ready	Treat as urgent. Begin Phase 1 immediately and consider specialist support.

Section scores matter as much as the total. A strong overall score with a No on breach readiness (questions 18 and 19) still leaves you exposed.

Domain	Questions	Max	Your score
A. Governance and accountability	1 to 5	10	
B. Notice and consent	6 to 11	12	
C. Rights of data principals	12 to 15	8	
D. Security and breach readiness	16 to 21	12	
E. Processors and cross-border	22 to 25	8	
F. Retention, erasure, accuracy, children	26 to 30	10	
Total	1 to 30	60	

5. Readiness roadmap

The plan below assumes a start in November 2026 and works back from 13 May 2027. If your timeline compresses, pull Phases 2 and 3 forward and run them in parallel.

Phase	Window	Key activities	Outputs
1. Mobilise and discover	Nov 2026	Appoint DPDP owner and working group. Brief leadership. Build the data inventory. Assess Significant Data Fiduciary status. Run the Section 3 assessment.	Owner named. Data map. Gap register. Budget.
2. Fix the foundations	Dec 2026 to Jan 2027	Redraft privacy notice. Redesign consent capture and withdrawal. Write the retention schedule. Define rights-request and grievance procedures.	Notice. Consent flow. Retention schedule. Rights SOP.
3. Secure systems and vendors	Jan to Mar 2027	Implement encryption, access control, logging (one-year retention). Update processor contracts. Map cross-border transfers. Review vendor assurance.	Control evidence. Signed processor terms. Vendor register.

Phase	Window	Key activities	Outputs
4. Prepare people and incidents	Mar to Apr 2027	Train staff. Publish grievance contact. Send notices for existing data where required. Run a breach drill including the 72-hour report.	Training records. Drill report. Published contact.
5. Verify and go live	Apr to 13 May 2027	Re-run the assessment. Fill gaps. Assemble the evidence file. Leadership sign-off.	Final score. Evidence file. Sign-off record.
6. Sustain	From May 2027	Annual review. Track MeitY guidance. Re-test breach plan. Audit processors yearly.	Annual review report.

6. Responsibilities matrix (RACI)

R = Responsible, A = Accountable, C = Consulted, I = Informed. Exec = leadership or board; DPDP lead includes a Data Protection Officer where appointed. Adjust the roles to match your organisation.

Activity	Exec	DPDP lead	Legal	IT/Sec	HR	Procure.
Appoint DPDP owner and budget	A	R	C	I	I	I
Data inventory and mapping	I	A	C	R	R	C
Privacy notice and consent design	I	A	R	C	C	I
Rights requests and grievances	I	A	C	R	R	I
Security safeguards and logging	I	C	I	A/R	I	I
Breach response and drills	A	R	R	R	C	I
Processor contracts and reviews	I	A	R	C	C	R
Retention and erasure	I	A	C	R	R	I
Training and awareness	I	A	C	C	R	I

7. Evidence register

Auditors, clients and the Data Protection Board will ask you to show your compliance, not describe it. Keep these items current.

Document or record	Shows that	Owner	Status
Data inventory and data flow map	You know what you hold and where it goes		
Privacy notice and version history	Notice is given and kept current		
Consent records and withdrawal log	Consent is obtained, evidenced and honoured		

Document or record	Shows that	Owner	Status
Rights and grievance register	Requests are logged and answered in time		
Security control evidence and log retention proof	Reasonable safeguards operate in practice		
Breach response plan and drill report	You can notify the Board and individuals		
Processor register and signed agreements	Vendors are bound and monitored		
Retention schedule and erasure logs	Data is deleted when the purpose ends		
Training records	Staff know their duties		
Significant Data Fiduciary assessment	You have considered the extra duties		

8. Addendum: hiring and background verification

Hiring and screening touch some of the most sensitive personal data an organisation holds: identity numbers, addresses, education and employment records. Use these additional checks if you run or buy background verification.

Check	Good practice
Consent	Capture digital, timestamped consent from each candidate, tied to each check, before verification starts.
Data minimisation	Use risk-based check packages by role. Do not run every check for every candidate.
Legitimate use	If you rely on the employment-related provision, document the purpose, limit data to what is needed and take legal advice.
Candidate rights	Give candidates a route to see, correct and dispute information in their report.
Vendor terms	Contract your verification provider as a processor: instructions, security, breach alerts, sub-processors, deletion.
Assurance	Ask for independent certifications (ISO 27001, SOC 2 Type II) and the provider's incident history process.
Retention	Set how long reports are kept. Confirm deletion at your provider and in your own inboxes and drives.
Cross-border checks	Map where candidate data travels when overseas education or employment is verified.

9. How Quinfy can help

Quinfy is an AI-native background verification company serving clients across more than 45 countries, and is certified to ISO 27001, ISO 9001 and SOC 2 Type II. If you would like help reviewing your hiring and verification workflows against this toolkit, we are glad to talk.

Quinfy Technology Pvt. Ltd.

541-542 Tower B3, Spaze I-Tech Park, Sector 49, Gurugram, Haryana 122018, India

Email: aashish.singh@quinfy.com | Phone: +91 98998 71303

© 2026 Quinfy Technology Pvt Ltd & Quinfy Inc. | All Rights Reserved. | This toolkit may be shared and used within your organisation. It is not legal advice.