SECURISTI

FREE READINESS TOOL · 2026 EDITION

The DPDPA Readiness Checklist.

A 40-point self-assessment for Data Fiduciaries against the Digital Personal Data Protection Act, 2023 and the DPDP Rules, 2025 — built from live engagements in regulated Indian sectors, not theory.

WHY NOW — THE COMMENCEMENT CLOCK (DPDP RULES, 2025 · G.S.R. 846(E))

13 NOV 2025	Rules published; Data Protection Board of India established
~13 NOV 2026	Consent Manager registration & obligations take effect (Rule 4)
~13 MAY 2027	Notice, security safeguards, breach reporting, children's data, SDF duties and data-principal rights become enforceable (Rules 3, 5–16)

Score yourself honestly. Every "No" is a workstream — and eighteen months disappears quickly.

Forty questions. Three answers each.

Work through each item with the people who actually operate the process — not just the policy owners. Mark each item Yes, Partial or No. The checklist covers ten obligation clusters drawn directly from the Act and the 2025 Rules; section and rule references are given so your counsel and auditors can trace every line back to the text.

SCORING GUIDE

32–40 Yes	Audit-hardened. Validate with an independent gap assessment and keep evidence live.
20–31 Yes	Directionally sound. Sequence the gaps against the 2026–27 commencement dates.
Below 20	Structural exposure. Penalties reach ₹250 crore per instance (Schedule, s.33). Start with lawful basis, notice and breach response.

This checklist is a readiness aid, not legal advice. Obligations marked with a commencement date are future-dated as at July 2026 — treat them as your build deadline.

Mark each item: Yes · Partial · No

A Lawful basis & governance

s.4–7 · s.8

Every processing activity is inventoried and tagged to consent (s.6) or a specific legitimate use (s.7) — nothing rests on an unwritten assumption.	☐ Y	☐ P	☐ N
You have confirmed you are not relying on GDPR-style ‘legitimate interests’ — a basis the DPDPA does not contain.	☐ Y	☐ P	☐ N
Accountability for DPDPA compliance is assigned at senior level, with a named contact person published for data principals (s.8(9)).	☐ Y	☐ P	☐ N
Personal data used for a decision affecting a data principal, or shared onward, is checked for completeness, accuracy and consistency (s.8(3)).	☐ Y	☐ P	☐ N

B Notice

s.5 · Rule 3 (in force ~May 2027)

A standalone, plain-language notice exists for every consent-based purpose — itemising the personal data and the specified purpose.	☐ Y	☐ P	☐ N
The notice gives working links to withdraw consent, exercise rights and complain to the Data Protection Board.	☐ Y	☐ P	☐ N
Notices are available in English and the Eighth-Schedule languages relevant to your data principals.	☐ Y	☐ P	☐ N
Legacy consents (pre-Act) have been identified and a re-notice plan exists (s.5(2)).	☐ Y	☐ P	☐ N

Mark each item: Yes · Partial · No

C Consent management

s.6 · Rule 4

Consent capture is a clear affirmative action — free, specific, informed, unconditional, unambiguous; no bundling, no pre-ticked boxes.	☐ Y	☐ P	☐ N
Withdrawal is as easy as giving consent (s.6(4)), and downstream processing stops within a defined SLA when it happens.	☐ Y	☐ P	☐ N
You retain demonstrable proof of every notice served and consent taken (s.6(10)) — queryable, not buried in logs.	☐ Y	☐ P	☐ N
You have assessed whether to integrate with registered Consent Managers ahead of Rule 4 commencement (~Nov 2026).	☐ Y	☐ P	☐ N

D Security safeguards

s.8(5) · Rule 6 (in force ~May 2027)

Personal data is protected by encryption, masking or tokenisation appropriate to the risk, in transit and at rest.	☐ Y	☐ P	☐ N
Access to personal data is role-based, reviewed periodically, and privileged access is logged.	☐ Y	☐ P	☐ N
Logs enabling detection and investigation of breaches are retained for a minimum of one year.	☐ Y	☐ P	☐ N
Backups exist for continuity of processing, and restoration is actually tested — not assumed.	☐ Y	☐ P	☐ N

Mark each item: Yes · Partial · No

E Breach detection & notification

s.8(6) · Rule 7 (in force ~May 2027)

A personal-data-breach runbook exists and is rehearsed — covering detection, triage, containment and communication.	☐ Y	☐ P	☐ N
You can notify each affected data principal without delay, in plain language, through their registered mode of communication.	☐ Y	☐ P	☐ N
You can file the initial Board intimation without delay and the full report within 72 hours — templates drafted, owners named.	☐ Y	☐ P	☐ N
Processor contracts obligate immediate breach escalation to you, with the information Rule 7 requires.	☐ Y	☐ P	☐ N

F Retention & erasure

s.8(7)–(8) · Rule 8

Retention periods are defined per purpose, and erasure actually executes — across production, backups and analytics copies.	☐ Y	☐ P	☐ N
Erasure triggers on consent withdrawal or when the specified purpose is served, whichever is earlier.	☐ Y	☐ P	☐ N
If you fall in a Third-Schedule class, the 48-hour pre-erasure notice to the data principal is built into the workflow.	☐ Y	☐ P	☐ N
You can evidence erasure by your processors on instruction (s.8(8)(b)).	☐ Y	☐ P	☐ N

Mark each item: Yes · Partial · No

G Processor governance

s.8(2) · Rule 6(2)

Every processor handling personal data operates under a valid written contract — no handshake arrangements.	☐ Y	☐ P	☐ N
Processor contracts flow down security-safeguard obligations equivalent to your own.	☐ Y	☐ P	☐ N
Third-party risk assessments cover DPDPA posture at onboarding and periodically thereafter.	☐ Y	☐ P	☐ N
You maintain a current register of processors, sub-processors and the data each touches.	☐ Y	☐ P	☐ N

H Children's & guardian data

s.9 · Rule 10 (in force ~May 2027)

You know whether you process data of persons under 18 — measured, not guessed.	☐ Y	☐ P	☐ N
Verifiable parental consent capture is designed for any child-facing processing.	☐ Y	☐ P	☐ N
No tracking, behavioural monitoring or targeted advertising is directed at children (s.9(3)).	☐ Y	☐ P	☐ N
Exemption applicability (Rule 10 / Fourth Schedule) has been formally assessed and documented.	☐ Y	☐ P	☐ N

Mark each item: Yes · Partial · No

I Data principal rights & grievance

s.11–14 · Rule 9, 13, 14 (in force ~May 2027)

Workflows exist for access, correction, completion, updating and erasure requests — with identity verification.	☐ Y	☐ P	☐ N
Grievances are acknowledged and resolved within your published timeline, inside the 90-day outer limit.	☐ Y	☐ P	☐ N
Data principals can nominate another individual to exercise rights on death or incapacity (s.14).	☐ Y	☐ P	☐ N
Rights channels are published in the notice and actually staffed — test them quarterly.	☐ Y	☐ P	☐ N

J SDF & cross-border readiness

s.10, s.16 · Rules 12–15

You have assessed whether Significant Data Fiduciary designation is likely for you — and what DPO-in-India, audit and DPIA duties would follow (s.10, Rule 13).	☐ Y	☐ P	☐ N
Annual DPIA and audit capability exists or is contracted, ready for SDF obligations.	☐ Y	☐ P	☐ N
Cross-border transfers are mapped; you can comply with any government restriction on transfer to notified countries (s.16, Rule 15).	☐ Y	☐ P	☐ N
If SDF-designated, you can comply with data-localisation directions for notified data classes (Rule 13(3)).	☐ Y	☐ P	☐ N

Counted your “No” answers?

Every gap on this list is a workstream Securisti has already built for regulated Indian businesses — notices and consent artefacts, breach runbooks rehearsed against the 72-hour clock, erasure that actually executes, and PIMS programmes aligned to ISO 27701. Bring us your completed checklist and we will turn it into a sequenced, costed roadmap against the May 2027 commencement date.

BOOK A 30-MINUTE DPDPA GAP REVIEW

support@securisti.com · www.securisti.com

B-116, Centrum Business Square, Waghle Estate, Thane West — 400604

D P D P A

SECURITY · ENGINEERED · BESPOKE