DPDPA Compliance: The 40-Point Checklist

A practical guide to obligations under India's Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 (DPDPA) applies to any organisation processing digital personal data in India, and to processing outside India connected with offering goods or services to individuals in India. Use this checklist to assess where your organisation stands.

A. Notice & Consent (Sections 5–7)

1. **Privacy notice in place** — Provide every Data Principal a clear notice before or at the time of requesting consent, describing the personal data collected and the purpose of processing.

2. **Itemised purposes** — List each purpose of processing separately in the notice; avoid vague, bundled, or open-ended purpose descriptions.

3. **Rights and grievance information in the notice** — The notice must explain how Data Principals can exercise their rights and how they can lodge a complaint with the Data Protection Board of India.

4. **Multilingual access** — Give Data Principals the option to access the notice in English or any of the 22 languages in the Eighth Schedule of the Constitution.

5. **Valid consent standard** — Ensure consent is free, specific, informed, unconditional and unambiguous, given through a clear affirmative action. Pre-ticked boxes and implied consent do not qualify.

6. **Purpose-limited consent** — Consent must be limited to personal data necessary for the specified purpose. Do not make consent for unnecessary data a condition of service.

7. **Easy withdrawal** — Make withdrawing consent as easy as giving it, and stop processing (and cause your processors to stop) once consent is withdrawn, subject to legal requirements.

8. **Legacy data notice** — For personal data collected before the Act with earlier consent, issue a fresh notice as soon as reasonably practicable.

9. **Consent Manager readiness** — Be prepared to honour consent given, managed, reviewed or withdrawn through a registered Consent Manager.

10. **Legitimate uses mapped** — Where you rely on "certain legitimate uses" (e.g., voluntary provision of data, employment purposes, medical emergencies, compliance with law), document which ground applies and why.

B. General Obligations of Data Fiduciaries (Section 8)

11. **Accountability for processors** — Remain responsible for compliance even where processing is done by a Data Processor on your behalf.

12. **Processor contracts** — Engage Data Processors only under a valid contract that governs the processing.

13. **Data accuracy** — Ensure completeness, accuracy and consistency of personal data used to make decisions affecting a Data Principal or disclosed to another Data Fiduciary.

14. **Reasonable security safeguards** — Implement appropriate technical and organisational measures (such as encryption, access controls, monitoring and logging) to prevent personal data breaches, including for data held by your processors.

15. **Breach notification** — On a personal data breach, notify the Data Protection Board of India and each affected Data Principal in the prescribed form and manner.

16. **Erasure on purpose completion** — Erase personal data (and cause processors to erase it) when consent is withdrawn or when the specified purpose is no longer being served, unless retention is required by law.

17. **Retention limits** — Define and enforce retention periods; do not keep personal data indefinitely "just in case." Track the specific retention timelines prescribed under the DPDP Rules for applicable classes of Data Fiduciaries.

18. **Published contact point** — Publish the business contact information of your Data Protection Officer (if applicable) or a person able to answer Data Principals' questions about processing.

19. **Grievance redressal mechanism** — Establish an effective, accessible mechanism to receive and respond to Data Principal grievances within the prescribed timelines.

20. **Government/State instrumentality data** — If processing data on behalf of the State or its instrumentalities, ensure compliance with the specific conditions applicable to such processing.

C. Children's & Persons with Disabilities' Data (Section 9)

21. **Verifiable parental consent** — Obtain verifiable consent of the parent or lawful guardian before processing personal data of a child (under 18) or a person with disability who has a lawful guardian.

22. **No detriment to children** — Do not undertake processing likely to cause any detrimental effect on the well-being of a child.

23. **No tracking or targeted ads at children** — Do not undertake tracking, behavioural monitoring of children, or targeted advertising directed at children, unless an exemption applies.

24. **Age-assurance process** — Implement a reliable method to identify child users and route them through the parental-consent flow, consistent with the DPDP Rules.

D. Significant Data Fiduciary Obligations (Section 10) — if notified as an SDF

25. **Appoint a DPO in India** — Appoint a Data Protection Officer based in India who represents the SDF, reports to the board or equivalent governing body, and serves as the point of contact for grievances.

26. **Independent data auditor** — Appoint an independent data auditor to evaluate DPDPA compliance.

27. **Data Protection Impact Assessments** — Conduct periodic DPIAs covering Data Principal rights, purposes of processing, risk assessment and mitigation measures.

28. **Periodic compliance audits** — Undertake periodic audits and other prescribed measures, and report as required under the DPDP Rules.

29. **Algorithmic due diligence** — Verify that algorithmic software deployed for processing does not pose a risk to the rights of Data Principals.

30. **Data localisation checks** — Monitor and comply with any government-specified restrictions on transferring particular categories of personal data outside India applicable to SDFs.

E. Data Principal Rights (Sections 11–14)

31. Right to access — Provide, on request, a summary of the personal data being processed, the processing activities, the identities of other Data Fiduciaries and Data Processors with whom data has been shared, and any other prescribed information.

32. Right to correction, completion, updating and erasure — Enable Data Principals to have their data corrected, completed, updated, and erased on request (subject to legal retention requirements).

33. Right to grievance redressal — Respond to grievances within the prescribed period; Data Principals must exhaust this mechanism before approaching the Data Protection Board.

34. Right to nominate — Allow Data Principals to nominate another individual to exercise their rights in the event of death or incapacity.

35. Simple rights-request channels — Publish clear, accessible means (e.g., a web form or email) for exercising each of these rights, and verify requester identity before acting.

F. Cross-Border Transfers & Restrictions (Section 16)

36. Restricted-country compliance — Track and comply with any Central Government notification restricting transfer of personal data to specified countries or territories.

37. Sectoral law overlay — Where sectoral laws (e.g., RBI, IRDAI, SEBI directions) impose stricter localisation or transfer conditions, comply with the higher standard.

G. Governance, Records & Ongoing Compliance

38. Data mapping and records — Maintain an up-to-date inventory of what personal data you collect, why, where it is stored, who accesses it, and with whom it is shared — including records of consents given and withdrawn.

39. Employee training and internal policies — Train staff on DPDPA obligations and adopt internal policies covering consent handling, breach response, retention, and rights requests.

40. Track the DPDP Rules and phased timelines — Monitor the Digital Personal Data Protection Rules, 2025 and their phased implementation deadlines, and align your compliance roadmap accordingly. Penalties for non-compliance can reach ■250 crore per instance.
