DPDP COMPLIANCE CHECKLIST

46 Point Tracker | Contract Audit | Model Processing Clause | India

HOW TO USE THIS CHECKLIST. Full DPDP obligations and penalties take effect in May 2027. Work through the sections in order, recording who owns each item. Section 4 is the contract audit, which is the part most organisations have not started and the part legal teams own. The model processing clause on page 5 can be dropped straight into vendor agreements.

The Three Dates

Date	What takes effect
November 2025	Data Protection Board of India constituted. Definitions and rule-making provisions in force. Penalty framework established.
November 2026	Consent Manager registration regime opens. Interoperable consent platforms.
May 2027	Notice and consent, security safeguards, data principal rights, breach notification, Significant Data Fiduciary duties, and PENALTIES up to Rs 250 crore.

Enforcement through 2026 is expected to focus on guidance rather than penalties. That is not a reason to wait. Phase 1 of any compliance programme, working out what data you actually hold, takes longer than every organisation budgets for and cannot be shortened by buying software.

Section 1 | Know What You Hold

Do this first. Everything else depends on it, and most organisations discover the answer differs by team.

✓	Obligation	Owner / status
☐	Data inventory completed: what personal data the organisation holds	
☐	Location of each dataset recorded, including cloud and third party systems	
☐	Purpose of collection documented for each dataset	
☐	Lawful basis identified: consent, or a legitimate use	
☐	Access list recorded: who inside the organisation can reach each dataset	
☐	Sharing map completed: every third party the data goes to	
☐	Retention period defined for each dataset	
☐	Children's data identified separately	
☐	Cross-border transfers identified	
☐	Shadow IT and unapproved AI tools audited	

Section 2 | Notice and Consent

✓	Obligation	Owner / status
☐	Standalone privacy notice drafted, separate from terms of service	
☐	Notice states the specific personal data collected	
☐	Notice states the specific purpose of processing	
☐	Notice explains how to exercise rights and how to complain to the Board	
☐	Notice available in English and the Eighth Schedule languages	
☐	Consent mechanism uses clear affirmative action, no pre-ticked boxes	
☐	Consent is unbundled, limited to what each purpose requires	
☐	Withdrawal is as easy as giving consent	
☐	Withdrawal triggers cessation of processing and erasure	
☐	Verifiable parental consent implemented for users under 18	
☐	No tracking, behavioural monitoring or targeted advertising to children	

Section 3 | Rights, Security and Breach

✓	Obligation	Owner / status
☐	Process for handling access requests, with a named owner	
☐	Process for correction and completion requests	
☐	Process for erasure requests	
☐	Grievance redressal contact published	
☐	Encryption in transit and at rest	
☐	Role-based access controls implemented	
☐	Logging and monitoring in place	
☐	Automated deletion workflow built for expired retention periods	
☐	Breach detection capability in place	
☐	Breach escalation path defined, with named decision maker	
☐	Breach notification templates pre-drafted for individuals and the Board	
☐	Simulated breach exercise run at least once	
☐	Data Protection Officer appointed and India-based, if a Significant Data Fiduciary	
☐	Data Protection Impact Assessment completed, if a Significant Data Fiduciary	
☐	Independent audit scheduled, if a Significant Data Fiduciary	

Section 4 | The Contract Audit

This is the section most organisations have not started. A processor has NO direct statutory obligations. The entire mechanism for controlling processor behaviour is contractual, and if the contract is silent the fiduciary carries the risk with no recourse.

✓	Obligation	Owner / status
☐	Contract register compiled: every agreement involving personal data	
☐	Vendor and supplier agreements reviewed	
☐	SaaS and cloud contracts reviewed, including provider standard terms	
☐	Consultancy and professional services agreements reviewed	
☐	Employment contracts reviewed	
☐	Marketing and analytics agreements reviewed	
☐	AI tool subscriptions reviewed, including any used without procurement approval	
☐	Each contract triaged: compliant, needs amendment, or needs replacement	
☐	Amendment programme scheduled with owners and dates	
☐	Negotiation position agreed for vendors who resist	

Model Data Processing Clause

Drop this into vendor, SaaS, consultancy and services agreements. Adapt the bracketed fields.

DATA PROTECTION

1. Definitions. "Personal Data", "Data Fiduciary", "Data Processor" and "Data Principal" have the meanings given in the Digital Personal Data Protection Act, 2023. In relation to Personal Data processed under this Agreement, the Customer is the Data Fiduciary and the Supplier is the Data Processor.

2. Purpose limitation. The Supplier shall process Personal Data only on the Customer's documented instructions and only to the extent necessary to provide the Services. The Supplier shall not process Personal Data for any other purpose, including its own product development, analytics or model training.

3. Security. The Supplier shall implement and maintain reasonable security safeguards appropriate to the risk, including encryption in transit and at rest, role-based access controls, logging, and measures to detect and address personal data breaches.

4. Personnel. The Supplier shall ensure that persons authorised to process Personal Data are bound by confidentiality obligations and receive appropriate training.

5. Sub-processing. The Supplier shall not engage any sub-processor without the Customer's prior written consent. Where consent is given, the Supplier shall impose obligations equivalent to this clause on the sub-processor and shall remain fully liable for its acts and omissions.

6. Breach notification. The Supplier shall notify the Customer of any personal data breach without undue delay and in any event within [twenty four] hours of becoming aware of it, and shall provide all information the Customer reasonably requires to meet its own notification obligations.

7. Assistance with rights. The Supplier shall provide reasonable assistance to enable the Customer to respond to requests from Data Principals to access, correct, complete or erase Personal Data, within [five] working days of the Customer's request.

8. Cross-border transfer. The Supplier shall not transfer Personal Data outside India without the Customer's prior written consent, and shall comply with any restriction notified by the Central Government.

9. Deletion on termination. On termination or expiry, the Supplier shall at the Customer's option delete or return all Personal Data and delete existing copies, and shall confirm compliance in writing within [thirty] days, save where retention is required by law.

10. Audit. The Supplier shall on reasonable notice permit the Customer or its appointed auditor to verify compliance with this clause, and shall provide such information as is reasonably required.

11. Indemnity. The Supplier shall indemnify the Customer against all losses, penalties, fines, costs and expenses arising from the Supplier's breach of this clause, including any penalty imposed by the Data Protection Board. This indemnity is NOT subject to the limitation of liability at clause [.....].

12. Survival. This clause shall survive termination or expiry of this Agreement.

Clause 11 is the one to fight for. Penalties attach to the FIDUCIARY, not the processor. Your vendor's failure becomes your penalty, so the indemnity has to sit outside the general liability cap or it is worthless against exposure of this scale. Clause 2 is the one vendors most often resist, because it stops them using your data for their own model training.

The 21 Month Sequence

- MONTHS 1 TO 3. Know what you hold. Data inventory, purposes, access, sharing, retention. This phase cannot be shortened and most organisations discover they do not know the answers.
- MONTHS 4 TO 9. Fix the paperwork. Privacy notice, consent architecture, retention schedule, breach response plan, and the processor contract programme. This is the phase legal teams own.
- MONTHS 10 TO 15. Build the systems. Consent capture and withdrawal, request handling, automated deletion, access controls, logging.
- MONTHS 16 TO 21. Test. Run a simulated breach and a simulated access request. Find out what fails while failure is still cheap.

Penalty Exposure

The Schedule sets maximum penalties by category of failure, reaching up to Rs 250 crore. Three points about exposure:

- CATEGORIES STACK. A single incident involving both a security failure and a notification failure attracts penalties under both heads. Cumulative exposure can exceed the headline figure substantially.
- PENALTIES ATTACH TO THE FIDUCIARY, not the processor. Your vendor's failure becomes your penalty. This is the entire argument for clause 11 above.
- THE BOARD CAN ACT ON COMPLAINT. A single disgruntled employee or customer can start the process. You do not need a headline breach to attract attention.

A note on scale. An EY survey of more than 150 professionals found close to 70 percent were not very familiar with the Act and Rules, and more than 81 percent had not updated or drafted DPDP-aligned contracts. If your organisation has not started, it is in the majority. That will not be a defence in May 2027.