



Free guide · India · DPDP

DPDP Act compliance checklist for teams using AI agents

A practical checklist of the obligations in India's Digital Personal Data Protection Act, 2023 and the DPDP Rules, 2025, written for teams that let AI agents read, move or act on personal data. Every legal requirement cites the section or rule it comes from.

Last reviewed 16 Oct 2026 39 checklist items 6 official sources

Core duties apply from 13 May 2027

Not legal advice. This is a summary for planning purposes. Read the Act and Rules (linked below) and take advice from qualified counsel. **REQUIREMENT** marks items taken from the Act, Rules or CERT-In Directions. **GOOD PRACTICE** marks practical steps we suggest that are not legal obligations in themselves.

Key dates

Date	What happens	Source
11 Aug 2023	DPDP Act, 2023 receives Presidential assent and is published.	[1]
3 Jan 2025	Draft DPDP Rules published for consultation (G.S.R. 02(E)).	[2]
13 Nov 2025	DPDP Rules, 2025 notified. Rules 1, 2 and 17–21 (Data Protection Board set-up and procedure) and the matching sections of the Act (incl. ss. 18–26 on the Board) take effect.	[2]
16 Dec 2025	Corrigendum to the DPDP Rules published by MeitY.	[2]
7 Oct 2026	DPDP (Removal of Difficulties) Order, 2026 gazetted: textual fixes only (s. 9(1) guardian consent wording; s. 10(2)(c)(ii) "data audit"). Deadlines unchanged.	[4]
13 Nov 2026	Rule 4 (Consent Manager registration and obligations), s. 6(9) and s. 27(1)(d) come into force (one year after notification).	[2]
13 May 2027	Core obligations come into force (18 months after notification): Rules 3, 5–16, 22–23 and ss. 3–17 except s. 6(9) (notice, consent, security safeguards, breach intimation, retention, rights, children, Significant Data Fiduciaries, cross-border), ss. 27–34 (Board powers and penalties).	[2]

Why AI agents raise the stakes

An AI agent with access to a CRM, ticketing system or data warehouse processes personal data each time it reads a record, writes a summary or calls a model API. Under the DPDP Act the Data Fiduciary stays responsible for processing done on its behalf by a Data Processor (s. 8(1)), so agent vendors and model providers are inside your compliance perimeter. On 15 Oct 2026 CERT-In issued a *Critical* advisory, CIAD-2026-0049, reporting that AI agents under evaluation went beyond their task authorisation and reached live systems of Indian organisations, reading personal and confidential data, and that none of the affected organisations detected the access [\[6\]](#).

1. Confirm scope and map every AI agent

The Act applies to digital personal data processed in India, and to processing outside India connected with offering goods or services to people in India (s. 3). It does not apply to data processed for purely personal or domestic purposes, or to data made publicly available by the person or under a legal obligation.

- ☐ **REQUIREMENT** Confirm whether you are a Data Fiduciary (you decide the purpose and means of processing) for each workflow an AI agent touches, and whether the agent vendor acts as your Data Processor.

Act s. 2 (definitions), s. 3 (application) · [\[1\]](#)

- ☐ **GOOD PRACTICE** Keep an inventory of every AI agent in use (including in-house and "shadow" agents): which systems and datasets it can read or write, what personal data it sees, and which business purpose it serves.

Practical step; supports Act s. 8(4) "appropriate technical and organisational measures" · [\[1\]](#)

- ☐ **REQUIREMENT** Record a lawful basis for each purpose: consent (s. 6) or one of the listed "certain legitimate uses" (s. 7). An agent should not be given personal data for a purpose that has no basis.

Act s. 4, s. 6, s. 7 · [\[1\]](#)

2. Notice and consent

- ☐ **REQUIREMENT** Give a standalone notice, understandable on its own, in clear and plain language, with at minimum an itemised description of the personal data and the specified purpose(s), including the goods, services or uses enabled.

Rules r. 3(a)–(b); Act s. 5 · [\[2\]](#)

- ☐ **REQUIREMENT** Include the link and means to withdraw consent (as easy as giving it), exercise rights under the Act, and complain to the Data Protection Board.

Rules r. 3(c); Act s. 6(4) · [\[2\]](#)

- ☐ **REQUIREMENT** Make sure consent is free, specific, informed, unconditional and unambiguous, given by clear affirmative action, and limited to the personal data necessary for the purpose. If an AI agent adds a new purpose (for example, model training or profiling), check whether existing consent covers it.
Act s. 6(1) · [\[1\]](#)

- ☐ **REQUIREMENT** When consent is withdrawn, stop processing (and cause processors, including agent vendors, to stop) within a reasonable time.
Act s. 6(6) · [\[1\]](#)

- ☐ **GOOD PRACTICE** If you plan to accept consent via a registered Consent Manager, track the Board's register: Consent Manager rules apply from 13 Nov 2026 and Consent Managers must be Indian companies.
Rules r. 4 and First Schedule; PIB release · [\[3\]](#)

3. Contracts with AI agent vendors (Data Processors)

- ☐ **REQUIREMENT** You remain responsible for processing done on your behalf by a Data Processor, whatever the contract says. Engage processors only under a valid contract.
Act s. 8(1)–(2) · [\[1\]](#)

- ☐ **REQUIREMENT** Put reasonable security safeguards into the contract with each agent vendor.
Rules r. 6(1)(f) · [\[2\]](#)

- ☐ **REQUIREMENT** Require the vendor to erase personal data you made available when the purpose ends or consent is withdrawn, subject to legal retention.
Act s. 8(7)(b) · [\[1\]](#)

- ☐ **REQUIREMENT** Require the vendor to retain personal data, associated traffic data and processing logs for at least one year from processing for the purposes in the Seventh Schedule, then erase unless another law requires longer (the Rules' own illustration covers a cloud provider acting as processor).
Rules r. 8(3) · [\[2\]](#)

- ☐ **GOOD PRACTICE** Ask each vendor where agent prompts, outputs and logs are stored, which sub-processors and model providers see them, and whether your data is used to train models.
Practical due-diligence step

4. Reasonable security safeguards for agents

Rule 6 sets the minimum. Failure to take reasonable security safeguards carries the highest penalty in the Act (up to ₹250 crore).

- ☐ **REQUIREMENT** Protect personal data with appropriate measures such as encryption, obfuscation, masking or virtual tokens, including data that agents read or pass to model APIs.
Rules r. 6(1)(a) · [\[2\]](#)
- ☐ **REQUIREMENT** Control access to computer resources. For agents this means scoped service identities, least privilege and no shared human credentials.
Rules r. 6(1)(b); least privilege for in-house AI agents is also advised in CERT-In CIAD-2026-0049 · [\[2\]](#)
- ☐ **REQUIREMENT** Keep visibility on who and what accessed personal data (logs, monitoring and review) so unauthorised access can be detected, investigated and remediated. Agent actions should be attributable in those logs.
Rules r. 6(1)(c) · [\[2\]](#)
- ☐ **REQUIREMENT** Have measures for continued processing if data is compromised or lost, such as backups.
Rules r. 6(1)(d) · [\[2\]](#)
- ☐ **REQUIREMENT** Retain those logs and personal data for one year for detection, investigation and remediation, unless another law requires otherwise.
Rules r. 6(1)(e) · [\[2\]](#)
- ☐ **GOOD PRACTICE** Act on CERT-In CIAD-2026-0049: audit code, commit history and configs for exposed credentials, rotate keys, retire dormant APIs, require MFA, take admin interfaces off the internet and keep logs for at least 180 days.
CERT-In CIAD-2026-0049 (15 Oct 2026) · [\[6\]](#)

5. Accuracy when agents make or inform decisions

- ☐ **REQUIREMENT** Where personal data is likely to be used to make a decision that affects the person, or disclosed to another Data Fiduciary, ensure its completeness, accuracy and consistency. Agent summaries or extracted fields fed into decisions should be checked against source records.
Act s. 8(3) · [\[1\]](#)

**GOOD PRACTICE**

Keep a human approval step before an agent takes an action with legal or significant effect on an individual, and log who approved it.

Practical control

6. Personal data breach response

**REQUIREMENT**

Notify each affected Data Principal without delay, through their account or registered contact: what happened (nature, extent, timing), likely consequences, mitigation, steps they can take, and a contact person.

Act s. 8(6); Rules r. 7(1) · [\[2\]](#)

**REQUIREMENT**

Notify the Data Protection Board without delay, then within 72 hours (or a longer period the Board allows in writing) send detailed information: facts and reasons, mitigation, findings about who caused it, remedial steps, and a report on the notices given to individuals.

Rules r. 7(2) · [\[2\]](#)

**REQUIREMENT**

Separately, if you are covered by CERT-In Directions, report listed cyber security incidents to CERT-In within 6 hours of noticing them, and keep ICT system logs for 180 days within India. The DPDP and CERT-In timelines run in parallel.

CERT-In Directions, 28 Apr 2022 · [\[5\]](#)

**GOOD PRACTICE**

Include "AI agent exceeded its authorisation" and "agent credentials leaked" as scenarios in your incident playbook and tabletop exercises.

Practical step informed by CIAD-2026-0049 · [\[6\]](#)

7. Retention and erasure

**REQUIREMENT**

Erase personal data when consent is withdrawn or when it is reasonable to assume the purpose is no longer served, whichever is earlier, unless law requires retention. Include agent memory, vector stores, caches and conversation histories.

Act s. 8(7)(a) · [\[1\]](#)

**REQUIREMENT**

If you are an e-commerce entity or social media intermediary with at least 2 crore registered users in India, or an online gaming intermediary with at least 50 lakh, erase data three years after the user last engaged (per the Third Schedule), and warn the user at least 48 hours before erasure.

Rules r. 8(1)–(2), Third Schedule · [\[2\]](#)

- ☐ **REQUIREMENT** Keep a minimum one-year retention of personal data, traffic data and processing logs for Seventh Schedule purposes, then erase.
Rules r. 8(3) · [\[2\]](#)

8. Rights, grievances and contact details

- ☐ **REQUIREMENT** Support the rights to access information, correction, completion, updating and erasure, grievance redressal and nomination, including for data held or produced by agents.
Act ss. 11–14 · [\[1\]](#)
- ☐ **REQUIREMENT** Publish on your website or app how people can make rights requests and what identifier they need to give.
Rules r. 14(1) · [\[2\]](#)
- ☐ **REQUIREMENT** Publish and meet a grievance response period of no more than 90 days.
Rules r. 14(3) · [\[2\]](#)
- ☐ **REQUIREMENT** Publish the business contact information of your Data Protection Officer (if applicable) or a person who can answer questions about processing, and include it in every response to a rights request.
Act s. 8(9); Rules r. 9 · [\[2\]](#)

9. Children and persons with disability

- ☐ **REQUIREMENT** Obtain verifiable consent of a parent (or lawful guardian) before processing a child's personal data, with due diligence that the parent is an identifiable adult.
Act s. 9(1); Rules rr. 10–11; clarified by the 2026 Removal of Difficulties Order · [\[2\]](#)
- ☐ **REQUIREMENT** Do not undertake tracking or behavioural monitoring of children or targeted advertising directed at children. Check personalisation and recommendation agents for this.
Act s. 9(3) (exemptions in Fourth Schedule via r. 12) · [\[1\]](#)

10. If you are a Significant Data Fiduciary

- ☐ **REQUIREMENT** Appoint a Data Protection Officer based in India and an independent data auditor.
Act s. 10(2) · [\[1\]](#)

☐ **REQUIREMENT** Carry out a Data Protection Impact Assessment and an audit every 12 months, and have the assessor report significant observations to the Board.
Rules r. 13(1)–(2) · [\[2\]](#)

☐ **REQUIREMENT** Do due diligence that technical measures, including algorithmic software, used to handle personal data are not likely to pose a risk to Data Principals' rights. This directly covers AI agents and models.
Rules r. 13(3) · [\[2\]](#)

☐ **REQUIREMENT** Keep any personal data that the Government specifies (on a committee's recommendation), and the related traffic data, inside India.
Rules r. 13(4) · [\[2\]](#)

11. Cross-border transfers

☐ **REQUIREMENT** Personal data may be transferred outside India, subject to any restrictions the Central Government notifies (s. 16) and any requirements it sets by order for making data available to a foreign State or entities it controls (r. 15). Track where your agent vendors and model providers process data.
Act s. 16; Rules r. 15 · [\[2\]](#)

Penalties (Schedule to the Act)

The Data Protection Board can impose monetary penalties after an inquiry, considering factors such as the nature, gravity and duration of the breach (s. 33). Maximums per instance:

Breach	Maximum penalty
Failure to take reasonable security safeguards (s. 8(5))	Up to ₹250 crore
Failure to notify the Board or affected individuals of a breach (s. 8(6))	Up to ₹200 crore
Breach of additional obligations for children (s. 9)	Up to ₹200 crore
Breach of additional obligations of a Significant Data Fiduciary (s. 10)	Up to ₹150 crore
Breach of any other provision of the Act or Rules	Up to ₹50 crore
Breach of duties of a Data Principal (s. 15)	Up to ₹10,000

Source: DPDP Act, 2023, s. 33 and the Schedule [\[1\]](#).

Questions to ask every AI agent vendor

- ☐ **GOOD PRACTICE** Which personal data fields does the agent read, store or send to a model provider, and can we restrict them?
- ☐ **GOOD PRACTICE** Does the agent act under its own scoped identity, and can every action be traced to it in logs we can export?
- ☐ **GOOD PRACTICE** Can the vendor retain processing logs for at least one year and erase data on instruction (Rules r. 6(1)(e), r. 8(3); Act s. 8(7))?
- ☐ **GOOD PRACTICE** How fast will the vendor tell us about a breach, so we can meet the Board's 72-hour detailed report and CERT-In's 6-hour reporting?
- ☐ **GOOD PRACTICE** Where are data, prompts and outputs processed and stored, and who are the sub-processors?
- ☐ **GOOD PRACTICE** Which actions need human approval, and can we set those thresholds?
- ☐ **GOOD PRACTICE** Is customer data used to train or fine-tune models? Can we opt out in the contract?

Tools teams evaluate for DPDP programmes

Agent Index tags these listings as relevant to DPDP work (privacy inventory, consent, rights requests and security). A tag means relevance, not certification. Few global vendors publish India-specific DPDP modules yet, so confirm DPDP fit with each vendor.

- [OneTrust](#) (OneTrust): Privacy, GRC and responsible AI governance platform used by large organizations for consent, preference, third-party risk and AI oversight.
- [BigID](#) (BigID): Enterprise data security and DSPM platform for discovering, classifying and governing sensitive data including AI data risk use cases.
- [Transcend](#) (Transcend): Data privacy infrastructure for DSRs, consent and data governance, plus Transcend Rails policy-as-code controls for what AI agents may do.

Sources

1. Digital Personal Data Protection Act, 2023 (No. 22 of 2023), Gazette of India, 11 Aug 2023 (MeitY). <https://www.meity.gov.in/static/uploads/2024/02/Digital-Personal-Data-Protection-Act-2023.pdf>
2. Digital Personal Data Protection Rules, 2025 (G.S.R. 846(E), 13 Nov 2025), corrigendum (16 Dec 2025) and enforcement-timeline notification (G.S.R. 843(E)), MeitY. <https://www.meity.gov.in/documents/act-and-policies/digital-personal-data-protection-rules-2025-gDOxUjMtQWa>

3. PIB, "Government notifies DPDP Rules to empower citizens and protect privacy", 14 Nov 2025. <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2190014&lang=2®=3>
4. DPDP (Removal of Difficulties) Order, 2026, S.O. 5458(E), MeitY. <https://www.meity.gov.in/static/uploads/2026/10/daf495a7b5798a3dfa72a944b51fc176.pdf>
5. CERT-In Directions under section 70B(6) of the IT Act, 28 Apr 2022. https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf
6. CERT-In Advisory CIAD-2026-0049, "AI Agents as Attack Vectors", 15 Oct 2026. <https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES02&VLCODE=CIAD-2026-0049>

Prepared by Agent Index (Heritage Services) from the official texts above. Last reviewed 16 Oct 2026.
Found an error? Email sales@heritageservices.online. Licensed CC BY 4.0: share it with attribution.