# DPDP Act Readiness Checklist

Nov 10, 2026 · @Vijay Srinivas Kothapalli

## Purpose and how to use this checklist

This checklist helps any organisation, large or small, check how ready it is for the Digital Personal Data Protection Act, 2023 and the DPDP Rules, 2025. Work through each item with the person who owns it, tick what is in place, and note the gaps.

- Tick an item only when you can show evidence, such as a signed policy, a system setting or a log.
- Items marked **Significant** apply only if the Central Government notifies you as a significant data fiduciary.
- Keep the checklist in your records. It is a self-assessment, not a certificate of compliance.

## Key timelines

The DPDP Rules were notified in November 2025, and obligations apply in phases. Confirm each date against the official Gazette text before relying on it.

| Milestone | Approximate date | What applies |
|---|---|---|
| Rules notified | 14 November 2025 | Start of the phased timeline |
| Consent manager framework | About 12 months after notification (November 2026) | Registration and operating rules for consent managers |
| Core obligations | About 18 months after notification (May 2027) | Consent notices, purpose limitation, children's data, retention and erasure, security safeguards |

(as of 10 November 2026)

## 1. Governance and roles

- [ ] A named person is accountable for data protection, with a deputy.
- [ ] Board or owner has reviewed the DPDP obligations and approved a plan.
- [ ] A written data protection policy covers collection, use, sharing, retention and deletion.
- [ ] A record lists the personal data you hold, its purpose, where it is stored and who can access it.
- [ ] Staff who handle personal data have been trained in the past 12 months.
- [ ] You have checked whether you process personal data of children or persons with disabilities, and whether you must treat it differently.
- [ ] You have assessed whether your scale or data sensitivity makes you a **Significant** data fiduciary.

## 2. Notice and consent

- [ ] Each collection point gives a clear notice in plain language, in English or the language the person uses.
- [ ] The notice states what data you collect, why, how long you keep it, and how the person can exercise their rights and complain to the Data Protection Board.
- [ ] Consent is free, specific, informed, unconditional and given by a clear affirmative action.
- [ ] Consent is not bundled with unrelated services.
- [ ] You record when and how consent was given, and can show it.
- [ ] Consent can be withdrawn as easily as it was given, and withdrawal is acted on promptly.
- [ ] Where you use a consent manager, you have confirmed that it is registered with the Board.

## 3. Rights of data principals

- [ ] A simple way exists to make a request: a form, email address or portal, with a published contact.
- [ ] You can confirm the identity of the person before acting on a request.
- [ ] Access requests are answered with a summary of the data and the processing.

- [ ] Correction and erasure requests are logged, actioned and confirmed to the person.
- [ ] Grievances are logged, with a named person responsible and a response timeline.
- [ ] Staff know how to recognise a request and where to send it.

## 4. Security, breach response and retention

- [ ] Access to personal data is limited to people who need it, and reviewed at least every quarter.
- [ ] Data is encrypted in storage and in transit, and backups are protected.
- [ ] Logs record access to personal data, and are kept and reviewed.
- [ ] A written incident response plan says who decides, who is told and how fast.
- [ ] You can detect and report a personal data breach to the Board and to affected persons, as the Rules require.
- [ ] You have a retention schedule for each category of data, and it is applied.
- [ ] Data no longer needed for its purpose is erased, unless a law requires you to keep it.

## 5. Processors, transfers and children's data

- [ ] Every vendor that processes personal data for you is listed, with a contract that requires the same protection.
- [ ] Contracts require the processor to delete or return data at the end of the engagement, and to report incidents promptly.
- [ ] Transfers of personal data outside India are checked against any restrictions the Central Government has notified.
- [ ] Before processing a child's data, you obtain verifiable parental consent, and do not track or target children.
- [ ] You have a process to stop processing that could cause harm to a child.
- [ ] **Significant** only: you have appointed a Data Protection Officer based in India and an independent data auditor, and you carry out periodic audits and impact assessments.

## Scoring your readiness

Count the ticked items in each section and add them up. The total is out of 31 items, excluding the two Significant-only items.

| Ticked items | Readiness | Next step |
|---|---|---|
| 24 or more | Well prepared | Keep evidence current, and review each year |
| 15 to 23 | Partly prepared | Close the unticked items in sections 1 and 4 first |
| Under 15 | Early stage | Appoint an owner, map your data and adopt a basic policy within 90 days |

Whatever the score, any unticked item in section 4 on breach response should be fixed before the core obligations date.

## About CRCO LLP

CRCO LLP is a Hyderabad-based advisory firm working on data privacy and protection, cybersecurity, outsourcing and process automation. We help organisations map their personal data, close readiness gaps and build the policies, notices and vendor controls the DPDP Act requires.

**Book a consultation:** visit the Contact page on our website, or write to us through the enquiry form.

*This checklist provides general guidance only. It is not legal advice. Check your obligations against the Act, the Rules and the Gazette text, and take advice for your own circumstances.*