§ DPDP — READINESS

The DPDP Readiness Checklist

A practical, section-by-section checklist for the Digital Personal Data Protection Act, 2023 — the working list we use to take a company from *unaware* to *defensible*. Built for the person handed “sort out DPDP” with no further instruction.

Forty checkpoints across eight areas. Print it, assign an owner to each line, and circulate it to your board and team.

HOW TO READ THIS · TICK WHAT IS TRUE TODAY · THE BLANKS ARE YOUR ROADMAP

§ 01

Know what data you hold

- ☐ Inventory every system, tool, and spreadsheet that holds personal data — HR, payroll, CRM, support, marketing, finance, vendor records.
- ☐ For each dataset, record the categories of personal data, whose data it is, and the purpose for holding it.
- ☐ Identify the source of each dataset and the lawful basis on which you hold it — consent or a permitted legitimate use.
- ☐ Note the retention period currently applied to each dataset, if any.
- ☐ Flag any data held without a current, identifiable purpose — it is a liability, not an asset.
- ☐ Map where you act as a Data Fiduciary and where you act as a Data Processor.

§ 02

Fix your notice and consent

- ☐ Review every point where you collect personal data — web forms, app sign-ups, paper forms, point of sale.
- ☐ Attach a plain-language notice stating what data is collected, for what purpose, and how rights are exercised.
- ☐ Remove pre-ticked boxes and bundled consent; consent for one purpose cannot be conditioned on an unrelated one.
- ☐ Build a mechanism to withdraw consent as easily as it was given — and act on withdrawal.
- ☐ Plan how you will issue fresh, compliant notice to Data Principals whose data you collected earlier.
- ☐ Keep a record of each consent obtained, with its timestamp and scope.

§ 03

Stand up the Data Principal rights workflow

- [ ] Establish a single intake channel for rights requests — access, correction, completion, erasure.
- [ ] Define the internal process: who receives, verifies identity, locates the data, acts, and responds.
- [ ] Build the capability to erase personal data once its purpose is served and no law requires retention.
- [ ] Define response timelines aligned to the Act and the rules framed under it.
- [ ] Support the right to nominate another individual to exercise rights on death or incapacity.

§ 04

Appoint the right accountable people

- [ ] Appoint a Grievance Officer and publish their contact details.
- [ ] Assess whether you are likely to be classified as a Significant Data Fiduciary.
- [ ] If so, appoint an India-based Data Protection Officer and plan periodic DPIAs and audits.
- [ ] Assign internal ownership for the data inventory, the rights workflow, and breach response.
- [ ] Document the basis for your Significant Data Fiduciary assessment, whichever way it lands.

§ 05

Bring your vendors and contracts into line

- [ ] Identify every third party that processes personal data on your behalf.
- [ ] Ensure each engagement is governed by a written contract binding the processor to your instructions.
- [ ] Maintain a register of sub-processors and the locations where data is processed.
- [ ] Where you act as a processor for your clients, reflect that role and its limits in your contracts.
- [ ] Confirm each processor contract requires appropriate security safeguards for the data.

§ 06

Prepare for a breach before you have one

- [ ] Document a breach response plan: detection, containment, assessment, notification, remediation.
- [ ] Define escalation — who declares a breach, who notifies, on what timeline.
- [ ] Prepare notification templates for the Data Protection Board of India and affected Data Principals.
- [ ] Run a tabletop test of the plan, and keep an incident log as evidence of diligence.

§ 07

Protect children's data and special cases

- ☐ Where you process the data of children, obtain verifiable consent of a parent or lawful guardian.
- ☐ Do not track, behaviourally monitor, or direct targeted advertising at children.
- ☐ If your service is not intended for children, state so and design collection to avoid gathering their data.
- ☐ Ensure any age-assurance approach is appropriate and proportionate, not excessive.

§ 08

Keep the evidence

- ☐ Retain your data inventory, notices, consent records, rights-request logs, vendor contracts, and breach logs.
- ☐ Date them, version them, and assign an owner to each record.
- ☐ Identify legal-hold or statutory retention obligations that override erasure.
- ☐ Store records so they can be produced on request — to an auditor, a board, or the Data Protection Board.
- ☐ Schedule a periodic review; readiness is a posture to maintain, not a project to finish.

Where this leaves you

Work through these eight areas and you move from a vague sense of exposure to a concrete, defensible position — one you can show a board, a buyer, or the Data Protection Board. If you would rather not run it alone, TruPath Compliance takes companies through every step of this checklist end-to-end.

START A READINESS REVIEW · INFO@TRUPATHCOMPLIANCE.COM · TRUPATHCOMPLIANCE.COM