FOUNTAINHEAD LEGAL

DATA PROTECTION LAWS OF INDIA

FREQUENTLY ASKED QUESTIONS FOR MANUFACTURING SECTOR



FOUNTAINHEAD LEGAL
C-2106, Oberoi Garden Estate, Chandivali Farm Road, Powai - 400076
T. +91 98338 62234 E. contact@fountainheadlegal.com
www.FountainheadLegal.com

UNDERSTAND THE BASICS

The Digital Personal Data Protection Act, 2023 and Rules, 2025 ("**DPDP Regulations**") govern digital records about people, from factory attendance to customer contacts.



1. We make products. Why does DPDP matter?

Your business also handles information about people. Review HR, contractors, factory visitors, product enquiries and service contacts, dealers, showrooms and delivery contacts.

2. What is personal data or PI?

Information that identifies a person. Examples include names, phone numbers, salaries, biometrics and identifiable CCTV footage. PI means Personal Information; DPDP Regulations use Personal Data. Organisational financials and production figures generally fall outside this definition unless linked to a person.

3. Who are the Data Principal, Fiduciary and Processor?

TERM	IN SIMPLE WORDS	EXAMPLE
Data Principal	The person the data concerns	An employee
Data Fiduciary	Decides why and how data is used	Your company for its own operations
Data Processor	Handles data on your behalf	A payroll provider following your instructions

4. What counts as processing?

Collecting, storing, viewing, using, sharing or deleting data. Emails, spreadsheets and business WhatsApp messages can contain personal data. Paper records enter scope when digitised.

5. When do we need to be ready?

Prepare by April 2027. Main obligations commence in May 2027. The November 2026 phase concerns Consent Managers; manufacturers do not have to appoint one simply because of that phase. Existing applicable privacy and cybersecurity requirements continue.

APPLY IT TO EVERYDAY WORK

6. Do we need consent for every employee record?

No. Check the purpose of each use. Certain employment-related uses, including payroll and specified employer protection purposes, can proceed without consent. Assess promotional photos and family information separately. Agency workers may not be your employees. For under-18s, check parental consent and applicable exceptions.

7. Can we keep CCTV and biometric attendance?

Review the purpose, legal basis, access and retention. Use clear CCTV signage and an accessible privacy explanation. For biometrics, check who stores the data and whether a less intrusive method meets the same need.

8. Can sales teams use customer and dealer contacts?

Use contacts for the purpose for which they were supplied. An enquiry contact can generally be used to respond, subject to DPDP Regulations. Assess unrelated campaigns, exhibition leads, purchased lists and WhatsApp marketing separately.

9. Is a website privacy policy enough?

No. Explain data use at the relevant interaction. Cover recruitment, factory entry and enquiries. A notice explains the use of data; consent records agreement where required. A notice alone does not obtain consent.

10.Can we share data within the group or overseas?

Group membership does not give unrestricted access. Companies should review head-office access and overseas support. Companies should map sharing across divisions, entities and shared systems. Overseas transfers must have a lawful basis and meet applicable restrictions. Foreign ownership alone does not create a separate category under the DPDP Regulations.

11.Which vendors need attention first?

Start with payroll, manpower, security, attendance, cloud and IT support. Identify the data shared and each vendor's role. Contracts should address permitted use, security, incidents, requests, retention and deletion. Your company remains responsible for its processing.

A USEFUL FIRST QUESTION - *Can you name the people, systems and vendors through which personal data enters your business? If not, start with data mapping.*

KNOW WHO DOES WHAT - READINESS

12. How long can we keep personal data?

Use a retention schedule for each type of record. Account for statutory records and the DPDP Regulations' minimum one-year requirements for relevant personal data and processing logs. Avoid indefinite storage and blanket deletion.

13.What security measures should we review?

Review who can access personal data, how it is protected, whether access is logged and monitored, and whether backups are available. Cover both your own systems and those operated by service providers.

14.What if someone asks about their data?

Publish a privacy contact and prepare a response process. Cover applicable access, correction, deletion and grievance requests. Verify identity, check legal retention requirements and record the response. HR, IT and vendors must know how to help.

15. What if data is lost or sent to the wrong person?

Escalate immediately as a potential personal data breach. Once the breach rules commence, notify affected individuals and the Data Protection Board without delay. Detailed Board reporting follows within **72 hours**, unless extended. Do not wait for head office to finish investigating.

CONTAIN → ESCALATE → ASSESS → NOTIFY → RECORD

16. Who should lead this and what is at stake?

Appoint a privacy lead supported by the business teams. Legal identifies permissible uses and documentation; IT implements controls; HR, Admin and Sales follow the processes. Security safeguard failures can attract penalties up to **INR 250 crore**. **These are maximum amounts, not automatic fines.**

YOUR PREPARATION PLAN

WHEN	PRIORITY	WHAT TO DO
Oct–Nov 2026	MAP	Map data, vendors and group access. Assign owners.
Dec 2026–Jan 2027	PREPARE	Finalise notices, policies, contracts and system changes.
Feb–Mar 2027	TEST	Implement controls, train teams and test a request and breach.
April 2027	CONFIRM	Close gaps and obtain management readiness sign-off.

Recommended project milestones, not separate statutory deadlines.

HOW FOUNTAINHEAD LEGAL SUPPORTS DPDP IMPLEMENTATION

DPDP implementation begins with understanding how your business uses personal data and identifying the requirements for each activity. We help establish this framework and work with your teams and technology partners to put it into practice.

A. Understand your data and identify gaps

We work with HR, IT, Admin, Sales and other teams to identify what personal data is collected, why it is used, where it is stored and who receives it. We assess gaps and prepare a practical implementation plan with priorities and responsibilities.

B. Prepare the framework

Our work covers:

- **Data use and consent:** Assess when consent is required, when another permitted basis applies, and how to handle employee, contractor, customer, visitor and children's data.
- **Notices and consent processes:** Prepare clear notices, consent wording and withdrawal processes suited to your business.
- **Vendor and group arrangements:** Review contracts and data sharing with service providers, group companies and overseas offices.
- **Policies and procedures:** Develop practical processes for retention, deletion, personal data breaches, individual rights and grievances.
- **Responsibilities and training:** Allocate responsibilities, train relevant teams and assess additional obligations where applicable.

Depending on the agreed scope, deliverables may include a gap assessment report, implementation tracker, data inventory, privacy notices, policies, contract amendments and training materials.

C. Support implementation by your technology teams

We translate the identified requirements into clear action points for your technology team or implementation partners. These may involve HR systems, websites, attendance systems, customer databases and vendor access. Technology teams can then configure consent capture, access permissions, security controls, logs, retention and deletion rules, and request handling workflows. We support the legal review of these changes and help resolve questions during implementation.

D. Help your teams manage ongoing compliance

Your internal teams and technology partners can manage day-to-day operations using the agreed framework. We can provide ongoing support for new vendors, business activities, data sharing arrangements, incidents and regulatory developments.

Build on a clear foundation

Clear decisions on consent, data use and retention help technology teams implement the right controls. We help establish these requirements at the outset, so your teams and partners can manage day-to-day compliance with greater clarity and less rework.

FOUNTAINHEAD LEGAL CONTACT DETAILS

To discuss DPDP implementation for your organisation, contact either of the following team members

rashmi@fountainheadlegal.com or + 91 98338 62234

shirin.patel@fountainheadlegal.com or + 91 98676 07153

aarushi@fountainheadlegal.com or + 91 91314 15290

***Disclaimer:** This handout is for general information only and does not constitute legal advice. Please seek specific legal advice before acting on its contents, as requirements may vary depending on your circumstances and changes in law.*