Manufacturing & Supply Chain

DPDPA 2023 Implementation Handbook

Digital Personal Data Protection Act, 2023 • India

For factories, logistics companies, warehousing, and supply chain management providers.

1. Overview & Applicability

Manufacturing and supply chain entities process personal data primarily of employees, contractual workers, vendors, and consignees. Factory biometric attendance systems, logistics driver tracking, and consignee delivery data are key compliance areas. While manufacturing is less data-intensive than tech or finance, the sheer size of the workforce — including contract and migrant labour — and the use of biometric access control systems make DPDPA compliance a priority.

2. Key Definitions Under DPDPA

These definitions govern how the Act applies to your sector:

Worker Data	Name, Aadhaar, PAN, health status, contractor affiliation, wage records — personal data of factory workers.
Biometric Attendance	Fingerprint/iris-based time and attendance for factory floors — sensitive biometric data.
Vendor Data	Contact persons, bank account details, GST credentials of supply chain vendors.
Consignee Data	Name, address, contact of final delivery recipients in logistics — personal data.
Tracking Data	GPS location of delivery vehicles and drivers — personal data of drivers.
Contract Labour	Data of workers employed through contractors requires consent — contractor is also a data processor.

3. Core Compliance Obligations

Every entity in this sector that processes personal data must comply with the following obligations:

1. **Worker Biometric Consent**
   Factory biometric attendance systems process sensitive data. Obtain written consent from every worker before enrolling. Provide alternative attendance for non-consenting workers.
2. **Contractual Worker Data**
   Workers engaged through labour contractors are still Data Principals. The contractor is a data processor — execute a DPA. The manufacturer remains responsible for data handling standards.
3. **Vendor Data Governance**
   Collect only necessary vendor contact and payment data. Store securely. Do not share with third parties without consent.
4. **Driver & Fleet Tracking**
   GPS tracking of delivery drivers is surveillance of personal data. Disclose tracking to drivers, obtain consent, and limit tracking to working hours only.
5. **Consignee Data**
   Delivery address and contact number of consignees must be used only for delivery purposes. Delete or anonymise after delivery completion.
6. **Health & Safety Records**
   Accident records, health screenings, and medical checkup data of workers — sensitive. Restrict access to HR and safety personnel only.

7	**Wage & Payroll Data** Wage records (especially for daily-wage and contract workers) containing bank details must be encrypted and access-controlled.

4. Implementation Checklist

Use this checklist to track your DPDPA compliance readiness:

- ☐ Obtain written biometric consent from all factory workers before enrolling in attendance systems.
- ☐ Execute DPAs with all labour contractors, logistics partners, and third-party warehousing companies.
- ☐ Implement encrypted storage for worker wage records, PAN, Aadhaar, and bank details.
- ☐ Disclose GPS tracking to all delivery drivers and obtain their consent — limit to working hours.
- ☐ Publish a privacy notice in Hindi and regional languages for factory workers.
- ☐ Build a worker rights mechanism — allow access to attendance records and wage slips, and correct errors.
- ☐ Appoint a Grievance Officer at the factory/plant level — communicate to workers during joining.
- ☐ Implement retention schedules — wage and attendance records must be deleted after statutory hold period.
- ☐ Train HR, safety, and operations teams on worker data handling obligations.
- ☐ Audit consignee data handling in logistics operations — implement post-delivery deletion protocols.

5. Applicable Penalties

The Data Protection Board of India (DPBI) may impose the following penalties for non-compliance:

Rs. 250 Crore	Failure to implement reasonable security safeguards resulting in a personal data breach
Rs. 200 Crore	Breach of obligations related to processing children's personal data
Rs. 150 Crore	Failure to fulfill obligations as a Significant Data Fiduciary (SDF)
Rs. 50 Crore	Failure to comply with Data Principal rights or other provisions of the Act

6. Implementation Roadmap

Follow this phased approach to achieve full DPDPA compliance:

1	**Month 1: Worker Data Inventory** Map all worker data — biometric, wage, health, contractor-sourced.
2	**Month 2: Consent Collection** Obtain written biometric and data processing consent from all current workers.
3	**Month 3: Contractor DPAs** Execute DPAs with all labour contractors and logistics service providers.
4	**Month 4: System Security** Encrypt biometric databases, wage records, and vendor data stores.
5	**Month 5: Rights & Grievance** Implement worker rights request mechanism; appoint plant-level Grievance Officer.
6	**Month 6+: Audit** Annual biometric consent audit and contractor data handling review.

🏭 Factory workers, especially migrant and contract labour, may not be aware of their data rights. Publish privacy notices in local languages and train your HR teams to explain rights clearly.