

Digital Personal Data Protection Rule 2025 - Industry Specific

09 February 2026 10:00 AM - 09 February 2026 05:30 PM

Brief Overview:

MADRAS MANAGEMENT ASSOCIATION

Presents

One day Workshop on

DIGITAL PERSONAL DATA PROTECTION RULES 2025- INDUSTRY SPECIFIC

Date :Monday, 9th February 2026

Time : 10:00 AM - 5:30 PM

Venue : Madras Management Center, Chennai.

This one-day workshop on the **Digital Personal Data Protection (DPDP) Rules, 2025** is designed to provide manufacturing organizations with a clear, practical, and implementation-oriented understanding of the new data protection regime. The program focuses on how DPDP applies to real-world manufacturing environments, covering employee data, contractor and vendor information, plant operations, and technology-driven systems such as HRMS, CCTV, attendance tools, and IoT-enabled smart factories.

A strong emphasis is placed on practical data mapping within manufacturing settings, enabling participants to trace data flows, classify digital personal data, and apply purpose limitation principles to daily operations. The session also covers implementation of DPDP frameworks, including consent and notice design, management of data principal rights, security and storage standards, and breach response obligations.

In addition, the workshop addresses vendor and supply chain risk management, audit readiness, and documentation requirements. Participants will leave with hands-on tools, ready-to-use templates, and a first-90-days action plan, helping reduce operational risk, ensure business continuity, and embed a culture of privacy across the organization.

Participants will gain clarity on the applicability of the DPDP Rules, key compliance timelines, and the

phased rollout covering notification, 12-month, and 18-month milestones. The workshop explains legal accountability, helping organizations understand their roles as data fiduciaries or data processors and how compliance responsibilities extend across staffing agencies, suppliers, and technology partners.

Session content:

- **DPDP Act, 2023 & DPDP Rules, 2025**

9:30 AM – 10:00 AM | Context Setting

Setting the Foundation for Privacy Compliance

- Why data protection and privacy matter for manufacturing organisations
- Evolution of India's data protection regime
- Shift from IT Act framework to the DPDP Act, 2023
- Sector-specific risks for manufacturing entities (HR data, vendor data, customer data, operational data)
- Overview of compliance expectations under the DPDP Rules, 2025

10:00 AM – 11:00 AM | Overview of the DPDP Act & DPDP Rules

Understanding the Legal Framework

- Key definitions and scope under the DPDP Act
- Applicability to manufacturing entities
- Roles and obligations of Data Fiduciaries and Data Processors
- Rights of Data Principals
- Penalties, enforcement mechanism and role of the Data Protection Board
- Key compliance timelines under the DPDP Rules, 2025

11:15 AM – 1:00 PM | Consent Framework under the DPDP Act

Consent, Notice & Consent Managers

- Meaning and standards of valid consent
- Notice requirements under the Act and Rules
- Layered notices and plain language drafting
- Role and functioning of Consent Managers
- Withdrawal of consent and its operational impact
- Special considerations for employee data and vendor data

Practical Exercise:

- Drafting a compliant consent notice for a manufacturing organisation
- Identifying scenarios where consent can be dropped or replaced with legitimate use

(including manufacturing-specific use cases)

1:00 PM – 2:00 PM | Lunch Break

2:00 PM – 3:00 PM | Data Security, Retention & Breach Preparedness

Operationalising Compliance

- Reasonable security safeguards under the DPDP Act
- Technical and organisational measures for manufacturing entities
- Data retention policies and lawful deletion
- Storage limitation and documentation requirements
- Preparing for data breaches: legal and operational readiness

3:00 PM – 3:15 PM | Data Breach & Incident Response

Regulatory and Practical Response

- What constitutes a personal data breach
- Breach notification requirements under the DPDP Rules
- Internal incident response workflows
- Coordination between legal, IT, HR and management
- Documentation and post-breach compliance

3:30 PM – 4:30 PM | Data Governance Framework

Building a Sustainable Privacy Program

- Data mapping and data inventory for manufacturing operations
- Data minimisation and purpose limitation
- Privacy by design and default
- Internal audits and compliance reviews
- Accountability mechanisms and record-keeping

Third-Party Management:

- Vendor risk assessment
- Data protection clauses in vendor contracts
- Structuring Data Processing Agreements (DPAs)
- Managing cross-functional accountability

4:30 PM onwards | Interactive Q&A Session

- Sector-specific compliance questions
- Practical challenges in implementation
- Clarifications on grey areas under the Act and Rules

For Whom:

- **Who Can Attend**

- This one-day program suits professionals from auto-ancillaries, heavy engineering, electronics assembly, food processing, and pharma manufacturing—who manage employee monitoring, IoT/smart factory data, vendor ecosystems, and compliance risks under the phased DPDP rollout (effective from Nov 2025).
- Ideal Roles and Seniority
- Focus on decision-makers and implementers with 5+ years experiences, who own HR/IT/operations budgets and report to plant heads or functional VPs:
- **Plant/Production Managers** (key for IoT/CCTV data flows, shift tracking compliance).
- **HR/Administration Heads**(handle employee PII, biometrics, attendance systems, contractor data).
- **IT/Cybersecurity Leads**(secure factory networks, vendor portals, breach response playbooks).
- **Supply Chain/Procurement Managers**(vendor DPAs, third-party risk assessments).
- **Compliance/Legal Officers** (DPIA coordination, Board audit prep for Significant Data Fiduciaries).

Key Takeaways:

Key Takeaways

Clarity on Legal and Compliance Requirements:

Understanding applicability: Clear awareness of how the Digital Personal Data Protection (DPDP) Rules 2025 apply specifically to manufacturing settings — including employee, vendor, and plant data. Compliance timelines: Knowledge of the staggered roll-out (notification, 12-month, and 18-month milestones) and when different categories of obligations, such as breach reporting and consent management, become mandatory.

Legal accountability: Recognition of the company's role as a data fiduciary vs. a data processor, and how liability extends to contractors, staffing agencies, and technology providers.

Practical Data Mapping for Manufacturing Environments.

Data flow identification: Ability to trace how personal data (of employees, contractors, and suppliers) moves within a plant and beyond — via HRMS, CCTV, IoT sensors, attendance systems, and vendor portals.

Classification frameworks: Categorizing data into sensitive vs. non-sensitive categories, determining

which data qualifies as digital personal data.

Minimal data principle: Understanding how to apply “purpose limitation” — collecting only what is needed to run operations, including shift scheduling or machine optimization.

Implementing DPDP Compliance Framework

Consent and notice design: Participants leave with templates for employee and vendor consent forms tailored to manufacturing operations (e.g., shift rostering, access control, safety tracking).

Right management systems: Clarity on how to operationalize data principal rights (access, correction, erasure) internally — including defined response times and escalation paths.

Security and storage standards: Knowledge of the technical safeguards required — encryption of IoT data, anonymization of production analytics, and secure retention/deletion rules.

Vendor and Supply Chain Risk Management

Third-party compliance controls: Participants gain an actionable checklist to assess vendor data handling capabilities before contract renewal or on boarding.

Model contract clauses: Familiarity with “DPDP-aligned” Data Processing Agreements (DPAs) and Standard Contractual Clauses for third-party and global vendors.

Audit-readiness: Understanding how to document compliance evidence (consent logs, DPIAs, and vendor audit trails) if inspected by the Data Protection Board.

Tools, Templates, and Action Plans

Practical toolkits: Hands-on templates such as:

- Data Inventory & Flow Mapping Sheet
- Breach Response Checklist (72-hour notification model)
- Factory IoT DPIA Format
- Employee Privacy Notice Template

First-90-days roadmap: Each participant drafts a personalized plan for their factory or organization, listing top 5 immediate and 5 medium-term compliance steps.

Risk Reduction and Business Value

Operational continuity: Understanding how proactive privacy measures reduce downtime, breach impact, and regulatory penalties.

Reputational trust: Positioning privacy compliance as a business differentiator, especially for exporters subject to global client audits or EU data regulations.

Cultural change: How to embed privacy awareness across plant supervisors, HR, IT, and contract workforce — turning compliance into an ongoing operational mind set.

These takeaways ensure that each participant not only understands the DPDP Rules 2025 but is ready to deploy a compliant privacy framework adapted to their manufacturing context.

Facilitator profile:

Fee Details:

- **Fee Details**
- Member amount : Rs 2950.00- (Including 18%GST)
- Non Member amount : Rs 3540.00- (Including 18%GST)
- Total Member count :