DPDP Rules 2025

A Practical **18-Month Data Protection Playbook** for **CHROs**

Turning employee data protection
into an operational advantage

**Perspective from the
CISO's Desk, Workmates**

EXECUTIVE SUMMARY

The Digital Personal Data Protection (DPDP) Rules introduce a new accountability framework for how organizations in India collect, process, store, and protect personal data. While compliance discussions often begin with Legal or IT, **HR functions are at the centre of DPDP impact.**

HR teams handle large volumes of sensitive employee data across recruitment, payroll, benefits, performance management, and separation. This data flows through multiple internal systems and external vendors, making HR one of the most exposed functions from a data protection standpoint.

DPDP compliance for HR is not a one-time exercise. It requires **structured execution over an 18-month horizon**, involving people, processes, technology, and governance.

This whitepaper presents:
- An HR-specific interpretation of DPDP requirements
- A practical employee data lifecycle framework
- A phased 18-month roadmap for CHROs
- Key risk areas and operational priorities
- Board-level considerations for sustained compliance

The intent is simple: help HR leaders move from uncertainty to **controlled, defensible, and auditable compliance**.

WORKMATES

WHY DPDP MATTERS TO HR LEADERS

HR is no longer a supporting function in data protection. Under DPDP, HR becomes a **core data fiduciary function**.

Employee data is:
- Highly sensitive
- Long-lived
- Shared across multiple vendors
- Accessed by multiple internal roles

Unlike customer data, employee data often lacks:
- Clear retention rules
- Consistent consent mechanisms
- Standardized access controls
- Periodic risk review

DPDP raises the bar from intent to **evidence**. Organizations must be able to demonstrate how employee data is governed, protected, and responded to when rights are exercised or incidents occur.

For CHROs, DPDP is not just a compliance obligation. It is a leadership test of **process maturity and governance discipline**.

DPDP THROUGH AN HR LENS: WHAT ACTUALLY CHANGES

DPDP introduces three practical shifts for HR operations:

Accountability becomes explicit

HR can no longer rely on informal practices or legacy processes.

Ownership for employee data handling must be defined, documented, and enforced.

Rights become operational

Employee rights related to access, correction, erasure, and grievance redressal must be handled through **defined workflows**, not ad-hoc responses.

Vendor failures become organizational failures

Background verification agencies, payroll partners, insurers, HR platforms, and wellness providers all fall within HR's data ecosystem.

Their lapses directly expose the organization.

DPDP compliance for HR is therefore about **operationalizing governance**, not drafting policies alone.
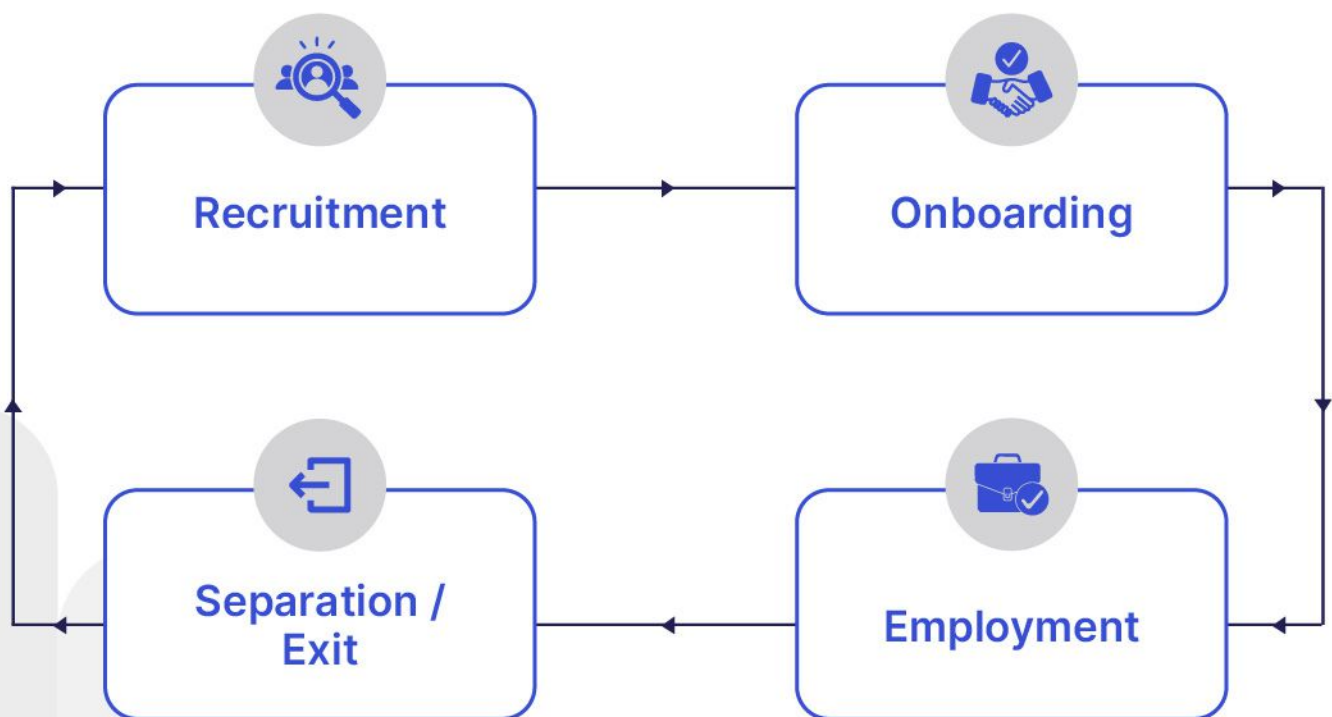
THE EMPLOYEE DATA LIFECYCLE FRAMEWORK

A lifecycle approach is the most effective way to structure HR compliance under DPDP.

Employee data typically flows through four stages:

Recruitment

Onboarding

Separation / Exit

Employment

Each stage involves different data types, risks, systems, and vendors. Treating DPDP as a lifecycle problem enables consistent controls and avoids fragmented compliance efforts.

WORKMATES

THE 18-MONTH HR COMPLIANCE ROADMAP

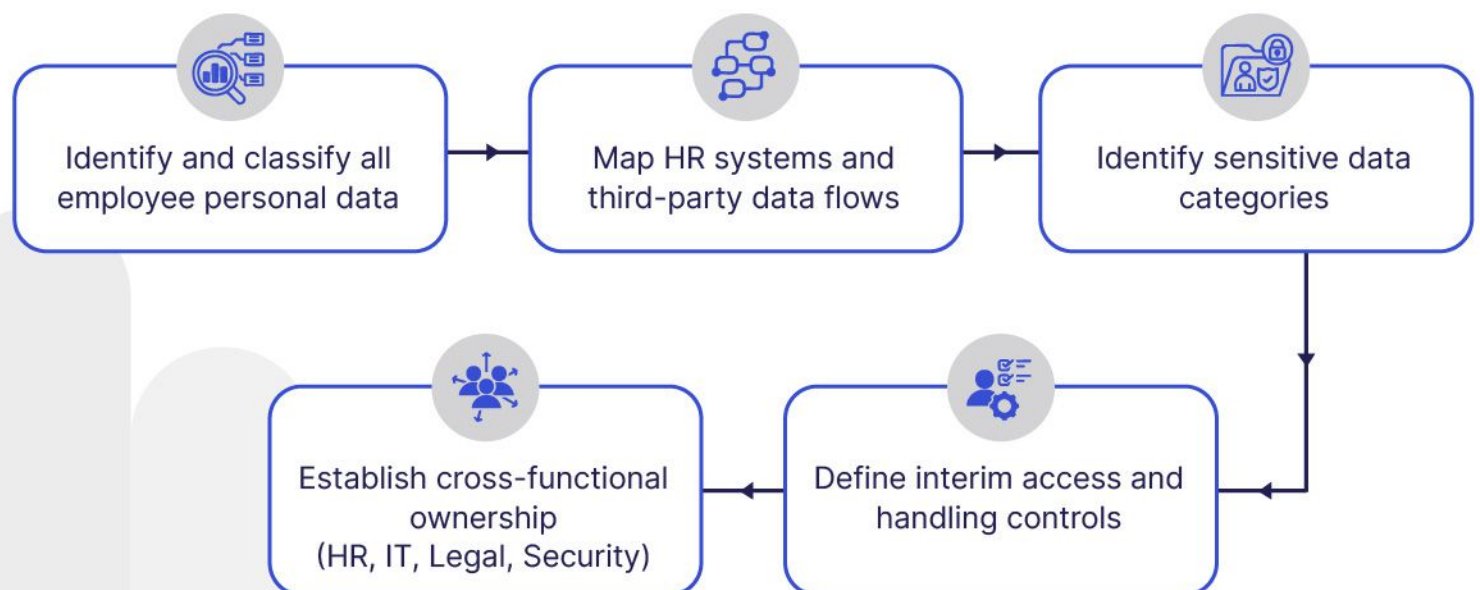DPDP implementation should be phased to ensure effectiveness and sustainability.

Phase 1: 0–3 Months
Foundation and Risk Visibility

Objective: Establish visibility and contain immediate risk.

Key HR actions

Identify and classify all employee personal data → Map HR systems and third-party data flows → Identify sensitive data categories

Establish cross-functional ownership (HR, IT, Legal, Security) ← Define interim access and handling controls

Outcome:
- Clear understanding of data exposure
- Prioritized risk areas
- Realistic remediation roadmap
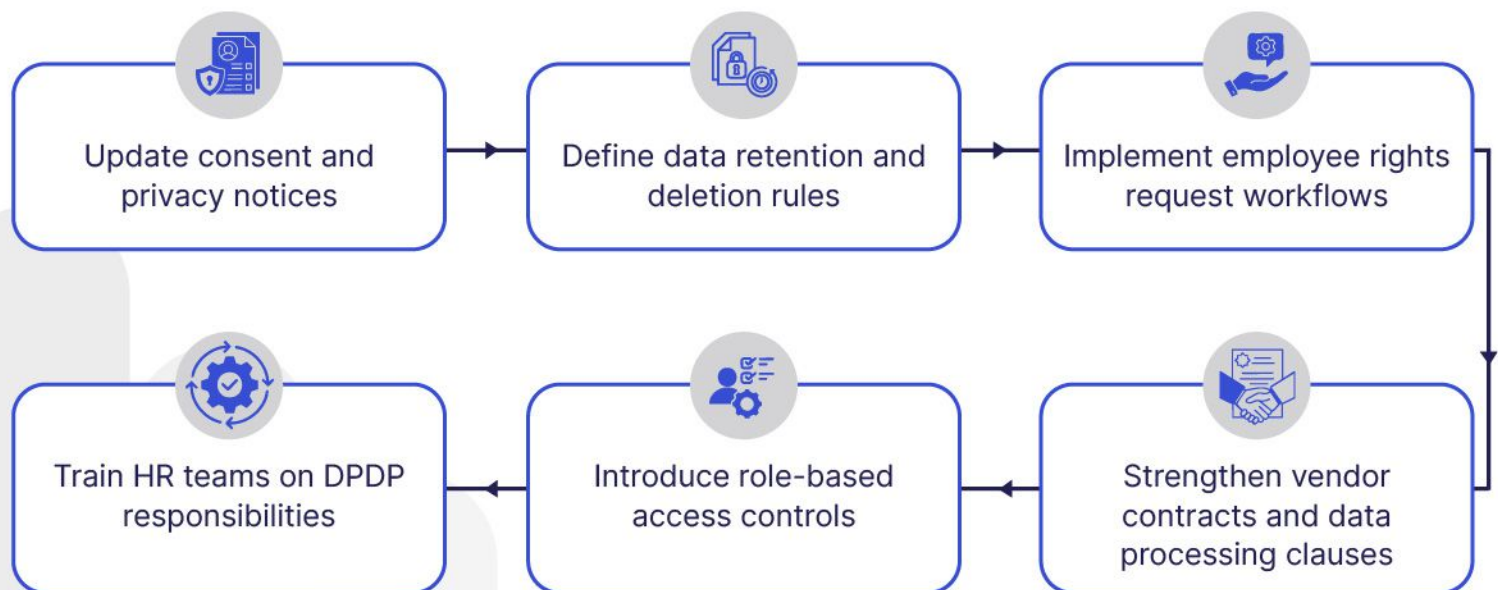
WORKMATES

THE 18-MONTH HR COMPLIANCE ROADMAP

DPDP implementation should be phased to ensure effectiveness and sustainability.

Phase 2: 3–9 Months
Process Standardization and Control Design

Objective: Build **repeatable** and **auditable** processes.

Key HR actions

```
Update consent and      →    Define data retention and    →    Implement employee rights
privacy notices              deletion rules                    request workflows

Train HR teams on DPDP  ←    Introduce role-based         ←    Strengthen vendor
responsibilities             access controls                   contracts and data
                                                               processing clauses
```

Outcome:
- Reduced dependency on individual judgment
- Consistent handling of employee data
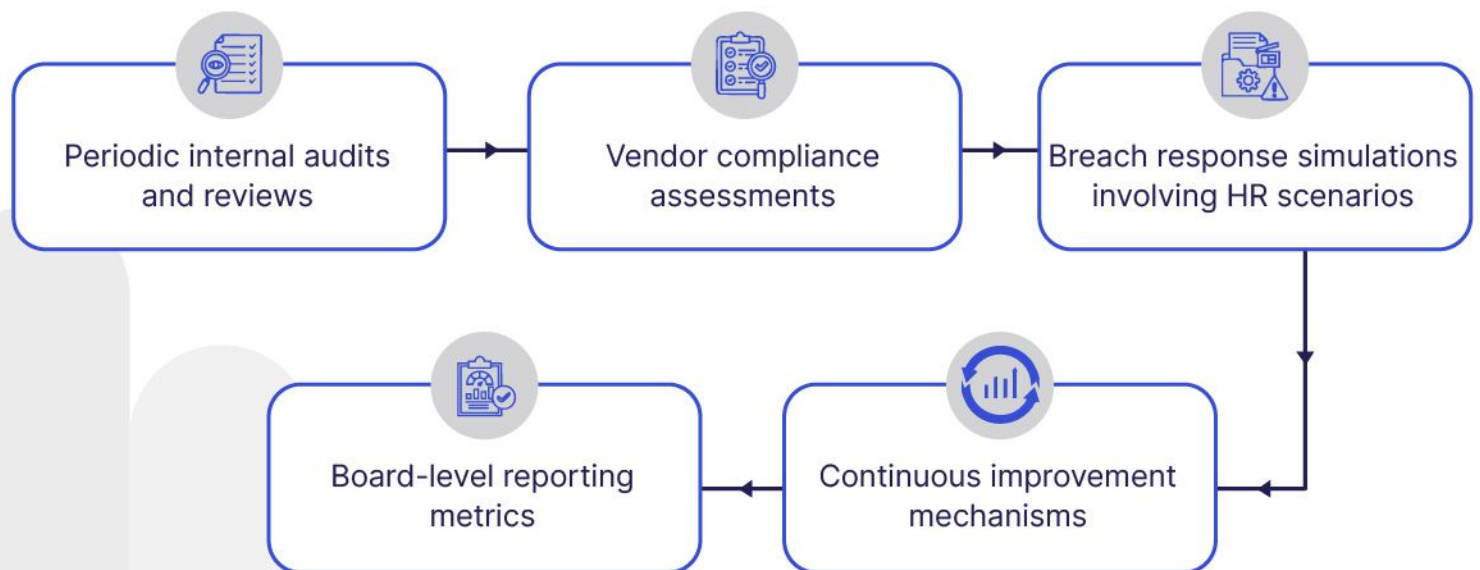- Improved audit readiness

THE 18-MONTH HR COMPLIANCE ROADMAP

DPDP implementation should be phased to ensure effectiveness and sustainability.

Phase 3: 9–18 Months
Operational Maturity and Governance

Objective: Embed compliance into day-to-day operations.

Key HR actions

```
Periodic internal audits  →  Vendor compliance  →  Breach response simulations
and reviews                  assessments            involving HR scenarios
                                                              ↓
Board-level reporting  ←  Continuous improvement  ←
metrics                   mechanisms
```

Outcome:
- Sustained compliance
- Leadership confidence
- Reduced regulatory and reputational risk

HIGH-RISK HR FUNCTIONS TO PRIORITIZE

While DPDP applies across HR, some functions carry higher risk:
- **Recruitment and background verification**
- **Payroll and compensation management**
- **Insurance, benefits, and wellness programs**
- **Grievances and disciplinary records**

Early focus on these areas delivers **disproportionate risk reduction**.

EMPLOYEE RIGHTS AND GRIEVANCE HANDLING

DPDP requires organizations to respond to employee data rights requests within defined timelines.

HR must enable:
- Request intake and authentication
- Coordination with IT and vendors
- Timely and documented responses
- Clear grievance escalation paths

This requires structured workflows, not informal coordination.

SECURITY AND BREACH PREPAREDNESS FOR HR DATA

HR data breaches have a unique impact due to the sensitivity of information and trust implications.

HR must be integrated into:
- Incident response planning
- Breach communication protocols
- Security awareness initiatives

"Reasonable safeguards" translate into **access controls, monitoring, vendor oversight, and preparedness drills**.

WHAT THE BOARD WILL EXPECT FROM HR

As DPDP matures, leadership and boards will seek visibility into:
- HR data risk posture
- Vendor compliance coverage
- Rights request volumes and resolution times
- Training completion rates
- Incident readiness indicators

CHROs who proactively report on these dimensions position HR as a g**overnance leader**, not a compliance laggard.

FROM COMPLIANCE TO CONFIDENCE

DPDP should not be approached as a regulatory burden alone.

For HR leaders, it is an opportunity to:
- Build employee trust
- Strengthen operational discipline
- Reduce long-term risk
- Enhance board credibility

The difference between compliance and chaos lies in **structured execution over time**.

CLOSING PERSPECTIVE

DPDP compliance for HR is a journey, not a milestone.

Organizations that adopt a lifecycle approach, phase execution thoughtfully, and align HR with IT and Security will move beyond compliance toward **resilient people data governance.**