INFOMAZE SPHERE

The DPDP Act Implementation Guide

for HR Teams.

A practitioner's guide to operationalising India's Digital Personal Data Protection Act, 2023 for HR data, vendors, and workflows.

A whitepaper from Sphere · 2026

infomazesphere.com

Executive summary

India's Digital Personal Data Protection Act, 2023 (DPDP Act) is in force. For HR teams, it is the most significant change to how employee data must be handled since the Information Technology Act, 2000. Yet the operational guidance available to HR practitioners is dominated by legal interpretations rather than implementation playbooks.

This guide is the implementation playbook. It is written for HR leaders, HR operations managers, and the IT teams supporting them — not for legal counsel. It assumes you have already accepted that the Act applies to you and now need to know what to do, in what order, by when.

In the pages that follow, we cover six foundational requirements that apply to every HR team under the Act; a phased five-stage implementation checklist with realistic timelines; fifteen questions to ask every HR software vendor before signing a contract; a reference list of clauses your Data Processing Agreement should contain; and the common pitfalls we see organisations fall into during implementation.

This guide is not legal advice. Decisions about how the Act applies to your specific situation should involve qualified counsel. What this guide provides is the operational shape of compliance — the parts that HR teams have to execute, regardless of how their lawyers interpret the edges.

Contents

01

What the DPDP Act is, in plain language

The Digital Personal Data Protection Act, 2023 is India's first comprehensive personal data protection law. It was passed by Parliament in August 2023 and is now in force, with rules and operational guidance continuing to roll out from the Ministry of Electronics and Information Technology.

In plain terms, the Act says four things that HR teams should internalise:

First, if you collect or process personal data of individuals in India, you must do so for a specific lawful purpose, and you must be able to demonstrate that purpose. The era of collecting employee data "just in case" — extended family details, optional documents not tied to any work requirement — is ending.

Second, the data principals (employees, in the HR context) have rights — to know what data you hold, to correct it, to have it erased when you no longer need it, and to nominate someone to exercise those rights if they cannot. These rights must be honoured within prescribed timeframes, through processes you can demonstrate.

Third, you are responsible for the data you hand to third parties. When your HR software vendor processes employee data on your behalf, you remain the data fiduciary. The vendor is a data processor. Your obligation does not transfer to them, but your contract must require them to meet equivalent standards.

Fourth, breaches must be reported. If a personal data breach occurs, you must notify the Data Protection Board and affected individuals — within timeframes specified in the rules.

Penalties for non-compliance can reach ■250 crore per breach, with materially lower amounts for specific lesser violations. The size of the penalty is set by the Data Protection Board based on the nature, gravity, and duration of the violation, the affected number of individuals, and whether the breach was preventable.

The Act applies to processing of digital personal data inside India. It also applies to processing outside India when that processing is connected to offering goods or services to individuals in India. For most Indian businesses, this means the Act applies, period.

> ***Why HR teams should read the Act before anyone else in the company does:*** *HR holds the broadest and most sensitive set of personal data in most organisations. Salaries, family details, medical information, performance records, identification documents, banking details. If a DPDP compliance project gets prioritised by data sensitivity, HR will be either the first workstream or the first thing that goes wrong if compliance is neglected.*

02

What HR data the Act covers

The DPDP Act defines personal data broadly as "any data about an individual who is identifiable by or in relation to such data." For HR purposes, this means essentially everything you hold about an employee, candidate, or alumnus.

A non-exhaustive list of what's clearly covered:

- **Identity and contact data:** name, photograph, address, phone, personal email, employee ID
- **Government identification:** PAN, Aadhaar (with additional protections), passport, driving licence
- **Compensation data:** salary structure, variable pay, bonuses, deductions, bank account details, UPI handles
- **Employment lifecycle data:** offer letters, appointment letters, performance reviews, promotion records, disciplinary actions, exit records
- **Family and dependent data:** spouse and dependent details, nominees, emergency contacts
- **Medical and health data:** medical insurance records, sick leave reasons, fitness for duty certificates, maternity records
- **Attendance and biometric data:** swipe records, biometric attendance scans, geolocation data from mobile attendance
- **Communication and behavioural data:** internal messages, performance commentary, surveys, exit interview content
- **Background verification data:** previous employment records, education verification, criminal background check results

Two specific categories warrant additional caution. **Children's data** (anyone under 18) requires verifiable parental consent and is restricted from being processed in ways that could cause harm. For HR teams, this affects internship programs involving school-age individuals and any handling of dependants' data where the dependants are minors.

Aadhaar data remains subject to the Aadhaar Act and its rules in addition to the DPDP Act. If your HR processes rely on Aadhaar — for verification, KYC, or any other purpose — you are subject to compounded compliance requirements and should treat Aadhaar handling as a distinct workstream in your implementation.

03

Six foundational requirements for HR teams

Beneath the legal text, the Act asks HR teams to internalise six operational principles. Every implementation project worth doing is structured around these. Here they are, each with the concrete HR-team obligation it creates.

3.1 Consent and notice

Personal data may only be processed for a specific purpose disclosed to the employee, with the employee's consent or under another lawful ground. Consent must be free, specific, informed, unconditional, and unambiguous — and revocable. "By signing this offer letter, you agree to the company processing your personal data" is not adequate consent.

Operational obligation: Build a consent and notice framework that clearly states the purpose of each data collection, gives employees a real choice where the Act permits, and tracks consent revocation. For most HR purposes (payroll, statutory compliance, employment contract performance), consent is not the lawful ground — "legitimate use" connected to employment is. But for purposes that step beyond that (marketing your services to employees, sharing data with third parties for non-employment purposes), explicit consent must be obtained.

3.2 Purpose limitation

Data collected for one purpose cannot be used for an unrelated purpose without fresh consent or another lawful ground. The shortcut of "we already have this data, let's use it for X" is no longer available.

Operational obligation: Maintain a registry of what data you collect, why, and what you're permitted to do with it. When a new HR initiative needs employee data (a new health screening program, a new performance analytics initiative, sharing data with an external survey vendor), check whether existing purposes cover it. If not, get fresh consent or establish a new lawful ground before proceeding.

3.3 Data minimisation

Only the data necessary for the stated purpose may be collected. The HR practice of asking for every possible piece of information on the onboarding form — "just in case" — is no longer defensible.

Operational obligation: Audit every form, every collection point, every data field. For each, ask: is this necessary for an actual employment-related purpose? If not, stop collecting it. This is one of the most operationally invasive requirements, because it forces you to redesign onboarding paperwork, employee profile forms, internal surveys, and exit interviews.

3.4 Retention

Personal data must not be retained beyond the period necessary for the purpose. "We keep everything forever" is no longer compliant. Some retention is required by other laws (tax records for seven years, for example) — those override the minimisation principle, but only for the data covered by those specific obligations.

Operational obligation: Establish a data retention schedule for every category of HR data. Common practice:

- Active employee data: held for the duration of employment plus the longer of (a) statutory retention requirements and (b) the limitation period for any claims arising from the employment
- Tax-related data (Form 16, TDS records, payslips): seven years per Income Tax Act
- PF/ESI records: five years per the respective statutes
- Candidate data (unsuccessful applicants): typically six months unless the candidate has explicitly consented to longer retention for future opportunities
- Background verification records: three years post-completion is a common compromise
- Exit interview content: indefinite retention is rarely defensible; eighteen to thirty-six months is more common

3.5 Rights of the data principal

Employees have specific, exercisable rights. The Act enumerates these:

- **Right of access:** employees can request a summary of the personal data you hold about them
- **Right of correction:** employees can require you to correct inaccurate or incomplete data
- **Right of erasure:** employees can require deletion of data no longer required for the stated purpose (subject to legal retention obligations)
- **Right of nomination:** employees can nominate someone to exercise these rights in case of death or incapacity
- **Right of grievance redressal:** employees can complain about how their data is handled, with a specific escalation path

Operational obligation: Build processes to receive, validate, and fulfil rights requests within timeframes that will be specified in the rules. Designate a Grievance Officer (mandatory under the Act). Train your HR team to recognise rights requests when they come in — they often arrive informally, embedded in resignation conversations or exit interviews, and get missed.

3.6 Security safeguards

Reasonable security safeguards must be in place. The Act does not prescribe specific controls but expects them to be appropriate to the nature, scale, and sensitivity of the data.

Operational obligation: Implement controls proportionate to the sensitivity of HR data. At a minimum: encrypted storage (data at rest), encrypted transmission (TLS), access controls limiting HR data to people with a need to know, audit logging of access to sensitive records, secure document handling for physical files, vendor security obligations in contracts.

04

Practical implementation checklist

DPDP compliance is not a project with a one-time end date. It's an operational change that embeds in how HR works, supported by an initial implementation that takes roughly six months for a well-resourced mid-market HR team. Here's a phased approach.

Phase 1: Audit (months 1-2)

- Inventory every category of personal data your HR team collects, processes, or stores
- Map every data flow — into your HR system, out to vendors, out to other internal teams, out to government portals
- Identify every third party with access to HR data (HRMS vendor, payroll vendor, background verification vendor, employee benefits providers, insurance brokers, auditors)
- Identify every legacy or shadow data source: spreadsheets HR maintains outside the HRMS, paper files, scanned documents in shared drives, employee data in Slack channels
- Identify the lawful ground for each processing purpose (employment contract, legal obligation, legitimate use, consent)
- Document the existing retention practice and where it deviates from defensible retention periods

Phase 2: Foundations (months 2-4)

- Draft and publish a Privacy Notice for employees, candidates, and alumni — clear, specific, and actually readable
- Establish your Grievance Officer role and publish their contact details
- Build a rights request intake and fulfilment process — even before requests start arriving
- Define retention schedules for every data category and document the rationale
- Update your offer letter, onboarding paperwork, and exit checklist to reflect new requirements
- Begin the data minimisation audit — identify forms and fields that collect data without a clear purpose

Phase 3: Vendor and contracts (months 3-5)

- List every HR-data-handling vendor and check whether they have a DPDP-compliant Data Processing Agreement
- Issue a DPA addendum to vendors that don't, with a defined response deadline
- Verify vendor security postures — request their SOC 2, ISO 27001 reports or equivalent assurance
- Document data flows to each vendor: what data they receive, what they do with it, where they store it, who they share it with
- Identify and address any cross-border data transfers; map them to the Act's transfer provisions

• Update vendor onboarding processes to make DPA execution a standard part of the procurement workflow

Phase 4: Process embedding (months 4-6)

• Train HR team members on data handling, rights requests, breach recognition, and escalation

• Train managers on data principles relevant to their work (giving feedback, performance discussions, references)

• Embed data protection considerations into HR system configuration: access controls, audit logging, retention automation

• Test the rights request fulfilment process with mock requests

• Establish the breach detection and notification process — including the 72-hour clock (or whatever the rules eventually specify)

• Communicate the changes to employees so they understand their rights and how to exercise them

Phase 5: Ongoing compliance

• Annual audit of data flows, vendor compliance, and retention adherence

• Quarterly review of any new HR initiatives for DPDP implications before launch

• Rights request metrics tracked and reviewed

• Vendor DPA renewals processed proactively

• Training refreshers annually for HR team, biennially for managers

• Incident response readiness reviewed quarterly

05

Fifteen questions to ask every HR vendor

Most of your DPDP exposure runs through your HR software vendor. The right contract and the right vendor capabilities make compliance manageable. The wrong choices make it nearly impossible. Before signing any new HR contract — or renewing an existing one — work through these fifteen questions with the vendor.

1. Data residency: Where is our employee data physically stored? Can we require it to stay in India?

2. DPA availability: Do you have a DPDP-compliant Data Processing Agreement ready to sign before contract execution?

3. Sub-processors: What sub-processors do you use, and where are they located? How will you notify us of changes?

4. Security certifications: Can you share your SOC 2 Type II report or ISO 27001 certification (or equivalent)?

5. Encryption: Is data encrypted at rest and in transit? With what standards?

6. Access controls: Who at your company has access to our employee data? Under what circumstances? Is there logging?

7. Audit logs: Can we get audit logs of who accessed which employee records, when, and from where?

8. Rights fulfilment: How does your platform support employee rights requests — access, correction, erasure?

9. Retention controls: Can we configure retention policies per data category, with automated deletion?

10. Data export: If we terminate the contract, in what format will our data be returned? How long do you retain it after termination?

11. Breach notification: What is your breach notification timeline to us? How will we be notified?

12. Cross-border transfers: Is any of our data transferred outside India? Under what mechanism (consent, SCCs, equivalent)?

13. AI / ML training: Is our employee data used to train your models, including for other customers? If so, under what controls?

14. Liability: What is your liability cap for data protection breaches? Does it carve out breaches caused by your negligence?

15. Grievance escalation: If we have a data protection grievance, who at your company handles it? What's the SLA?

How to use these questions in practice: *Send them in writing before final commercial negotiation. A vendor that takes more than ten business days to provide written answers is signalling something about how their DPDP work is going internally. Vendors that answer in writing within a few days, with cited specifics, are usually further along.*

06

What your Data Processing Agreement should contain

Your DPA with each HR-data-handling vendor is the contractual backbone of your compliance posture. It defines what the vendor is allowed and required to do with your employee data. A DPDP-aligned DPA should contain the following clauses, at minimum.

Roles and definitions. Clear identification of you as the Data Fiduciary and the vendor as the Data Processor. Reference to the DPDP Act.

Scope of processing. Detailed description of what data is processed, for what purposes, on what instructions.

Vendor obligations. Vendor will process data only on documented instructions, will not use data for its own purposes, will not disclose data to third parties except as instructed.

Confidentiality. Vendor personnel processing the data are bound by confidentiality obligations equivalent to those in your DPA.

Security measures. Specific security measures the vendor will implement (encryption standards, access controls, audit logging, vulnerability management). Avoid 'industry standard' — name the controls.

Sub-processors. Notification requirements before engaging new sub-processors, your right to object, sub-processor list available on request.

Data subject rights. Vendor will support you in responding to rights requests, with defined timeframes for their assistance.

Breach notification. Vendor will notify you within a specified time (commonly 24-48 hours) of becoming aware of any personal data breach affecting your data. Specify required content of the notification.

Cross-border transfers. If transfers occur, the mechanism used. Notification to you before any new transfer destination is added.

Audit rights. Your right to audit (directly or via a third party) the vendor's compliance with the DPA, with reasonable notice and frequency limits.

Data return and deletion. On termination, vendor returns or deletes all customer data within a defined period (commonly 30-60 days). Written certification of deletion.

Liability. Liability for breaches of the DPA, including indemnification for fines or claims arising from the vendor's non-compliance.

Survival. Confidentiality, return/deletion, and liability provisions survive termination.

Important practical note: *Most vendors provide a standard DPA template. Read it carefully. Standard templates are usually written from the vendor's perspective and may shift more risk to you than is necessary. Negotiate at least the breach notification timeline, the sub-processor notification process, audit rights, and liability terms. Vendors who refuse to negotiate any of these are signalling something about how they think about your data.*

07

Common pitfalls and how to avoid them

Treating DPDP as a one-time project.

DPDP compliance is operational, not project-based. Teams that treat the initial six-month implementation as the end state find themselves out of compliance again within a year as new HR initiatives are launched without DPDP review. Embed DPDP review into the HR change-management process from day one.

Underestimating shadow data.

Almost every HR team has employee data outside the HRMS — spreadsheets one manager keeps, scanned documents in Drive folders, employee details in Slack messages, candidate notes in personal note apps. These are subject to DPDP just as the HRMS data is. Your audit must include them, and your processes must address them.

Vague vendor DPAs.

Vendor DPAs that say 'we will implement appropriate security measures' without specifics are worth less than vendor DPAs that name specific controls. Push back on vagueness. Vagueness benefits the vendor and harms you when something goes wrong.

Missing the breach clock.

If your breach detection takes 72 hours and your notification timeline is 72 hours, you have zero margin. Build detection capability that surfaces incidents within hours, not days. Make sure your vendors do too — their breach is your breach, and the clock starts when they discover it, not when they tell you.

Over-collecting on onboarding.

The single most common DPDP problem we see is HR onboarding forms that haven't been audited in years. They collect spouse's blood group, references' email addresses, ancestral village names — none of which serves a defensible employment purpose. Audit and prune.

Ignoring data principal rights until they arrive.

Many teams plan to 'figure out the rights process when we get our first request.' By then the request is already running against a clock. Build the intake form, the validation workflow, and the fulfilment process before the first request arrives. Test it with a mock.

Confusing 'legitimate use' with 'we can do anything'.

Legitimate use is a real lawful ground under the Act, but it has limits. Processing necessary for the employment contract is legitimate. Sharing employee data with a third party for marketing is not, even if you 'employ' them. Don't stretch the concept past where it actually fits.

Cross-border transfer assumptions.

Many HR products are hosted outside India by default. If yours is, that's a cross-border transfer that needs a lawful basis. Don't assume your vendor has handled this — check, ask for the transfer mechanism in writing, and decide whether to require Indian hosting.

08

About Infomaze Sphere and HRPLANR

Infomaze Sphere is the product division of the Infomaze group, a software services company with fifteen-plus years of experience building operational software for businesses across India and globally. Sphere productises the patterns we've seen repeatedly across customer engagements, shipping focused SaaS products for specific operational problems.

Our portfolio includes PrintPLANR (print management), FieldPLANR (field service operations), QuotePLANR (configurable quoting), HRPLANR (workforce operations), and ANSWR (AI agents for customer interaction).

HRPLANR

HRPLANR is our workforce operations platform, built India-first. DPDP compliance is a first-class design priority, not a bolted-on module. India statutory compliance is native — PF, ESI, Professional Tax across all 21 states, quarterly TDS, annual Form 16, gratuity, POSH returns, the Maternity Benefit Act. AI is built in, not bolted on. The free tier (up to 10 employees, forever) means the smallest startup can run compliantly from day one.

If this guide has been useful, HRPLANR may be useful to your evaluation. Visit infomazesphere.com/products/hrplanr-hr-software for the product overview, or hrplanr.com for the full product website.

Talk to us

hello@infomazesphere.com
privacy@infomazesphere.com (privacy specifically)
infomazesphere.com

This whitepaper is a practitioner's guide. It is not legal advice. Decisions about how the DPDP Act applies to your specific situation should involve qualified legal counsel.