👥 HR, Staffing & Recruitment

DPDPA 2023 Implementation Handbook

Digital Personal Data Protection Act, 2023 • India

For employers, HR departments, job portals, recruitment agencies, staffing firms, and payroll SaaS providers.

1. Overview & Applicability

HR and recruitment entities process some of the most sensitive personal data — financial information, health status, criminal records, biometric attendance, performance evaluations, and salary details. The DPDPA requires employers to treat employee data with the same care as customer data. Recruitment platforms hold vast databases of candidate CVs and assessment results that require strong governance. Biometric attendance systems require explicit employee consent.

2. Key Definitions Under DPDPA

These definitions govern how the Act applies to your sector:

Employee Data	Name, address, PAN, Aadhaar, salary, health status, performance records, disciplinary history — personal data.
Candidate Data	CV, assessment results, interview notes, background verification — personal data collected during recruitment.
Biometric Data	Fingerprint or facial recognition used for attendance — sensitive data requiring explicit consent.
Health Data	Medical certificates, maternity records, disability disclosures — sensitive health data.
Background Verification	Criminal record checks, credit history — requires explicit candidate consent before initiation.
Data Processor	Payroll software, HRMS providers, background verification agencies — require DPAs.

3. Core Compliance Obligations

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

1. **Employee Consent at Onboarding**
   Obtain DPDPA-compliant consent from employees at onboarding for all data processing purposes — payroll, performance management, health benefits, biometric attendance. Each purpose needs separate consent.
2. **Biometric Attendance**
   Fingerprint and facial recognition attendance systems process sensitive biometric data. Obtain explicit written consent. Provide an alternative attendance method for those who refuse.
3. **Candidate Data Governance**
   CVs and assessment data should be retained only for the recruitment cycle plus a defined hold period. Send rejection notifications and delete data thereafter.
4. **Background Verification**
   Obtain explicit candidate consent before initiating any background verification. Share only the minimum necessary data with verification agencies (execute DPAs).
5. **Payroll Data Security**
   Payroll data (salary, PAN, bank account) must be encrypted. Access restricted to payroll team with audit logs.
6. **Performance & Disciplinary Records**
   Do not share performance evaluations or disciplinary records with third parties without employee consent. Retain only as long as necessary.

7	**Job Portal Obligations** Job portals holding candidate databases must implement strong access controls, obtain consent for profile sharing, and allow candidates to download and delete their profiles.
8	**Termination Data Handling** On employee departure, delete or anonymise personal data per defined retention schedule. Issue a data return/deletion notice to the employee.

4. Implementation Checklist

Use this checklist to track your DPDPA compliance readiness:

- ☐ Update employment contracts and onboarding forms to include DPDPA-compliant consent clauses.
- ☐ Obtain separate, explicit consent for biometric attendance — provide an alternative for non-consenting employees.
- ☐ Audit candidate data — set retention periods and implement automated deletion after recruitment cycle.
- ☐ Execute DPAs with background verification agencies, payroll software providers, and HRMS vendors.
- ☐ Implement encrypted storage for payroll data (salary, PAN, bank account details).
- ☐ Build an employee rights portal — allow access to personal file, correction requests, and payslip downloads.
- ☐ Appoint a Grievance Officer (may be HR Head) and communicate contact details to all employees.
- ☐ Implement a candidate rejection and data deletion protocol — notify rejected candidates and delete CVs.
- ☐ Review health data handling — medical certificates and disability data must have restricted access.
- ☐ Train HR teams and recruiters on DPDPA obligations and data handling best practices.
- ☐ Conduct an annual HRMS and payroll vendor audit — review DPAs and security practices.
- ☐ Establish a clear termination data handling procedure and include it in the exit policy.

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: HR Data Inventory** Map all employee and candidate data — what is collected, stored, shared, and for how long.
2	**Month 2: Consent Overhaul** Redesign onboarding consent forms and candidate consent processes.
3	**Month 3: Biometric Compliance** Review biometric attendance systems — obtain fresh consent or implement alternatives.
4	**Month 4: Vendor DPAs** Execute DPAs with all HR tech vendors, payroll providers, and background verification agencies.
5	**Month 5: Rights & Grievance** Build employee rights portal and appoint/train Grievance Officer.

6 **Month 6+: Annual Review**

Annual HR data audit and consent record review.

👔 Employees are Data Principals too. Their consent to biometric collection, performance monitoring, and health data processing must be freely given — not coerced as a condition of employment.