

EMPLOYEE PRIVACY NOTICE

Under the Digital Personal Data Protection Act, 2023

DPDPA Legal | Roots Cyber Law Firm | Template Form 03

DISCLAIMER: This form template is prepared by DPDPA Legal, managed by Roots Cyber Law Firm, for compliance guidance under the Digital Personal Data Protection Act, 2023. It does not constitute legal advice. Consult qualified legal counsel before deployment.

Dear Employee,

This Employee Privacy Notice explains how **[Organisation Name]** ("Company", "we", "us") collects, uses, stores, and protects your personal data in accordance with the **Digital Personal Data Protection Act, 2023 (DPDPA)**.

1. PERSONAL DATA WE COLLECT

Identity details	Name, date of birth, photograph
Contact details	Address, phone number, email, emergency contacts
Employment information	Employee ID, designation, department, joining/exit dates, previous employment
Payroll & financial data	Bank details, salary information, tax declarations
Statutory data	PAN, Aadhaar (masked), PF/UAN/ESIC, passport or visa (where applicable)
Attendance & access data	Attendance records, access card or biometric logs
IT & system usage data	Official email usage, device and network logs
Performance & HR records	Appraisals, training records, disciplinary actions
Health & safety data	Medical fitness or insurance details, where required by law

2. PURPOSE OF PROCESSING

- ◆ Recruitment, onboarding, and employment administration
- ◆ Payroll processing and statutory compliance (PF, ESI, Income Tax, Gratuity)
- ◆ Workforce management, attendance, and performance evaluation
- ◆ IT security, system access control, and fraud prevention
- ◆ Health, safety, and insurance administration
- ◆ Compliance with labour, tax, and other applicable laws
- ◆ Internal audits, investigations, and grievance handling

3. LAWFUL BASIS FOR PROCESSING

Processing Activity	Lawful Basis under DPDPA
Employment contract administration & payroll	Performance of employment contract / Legitimate use
Statutory compliance (PF, TDS, ESIC)	Legal obligation
IT system monitoring & security	Legitimate use
Optional wellness or benefit programmes	Consent

4. DATA SHARING

- ◆ Internal teams on a need-to-know basis
- ◆ Authorised service providers (HRMS, payroll, IT support, insurers)
- ◆ Government authorities or regulators where legally required
- ◆ All third parties are required to maintain appropriate data protection safeguards

5. DATA RETENTION

- ◆ Personal data retained only for as long as necessary to fulfil the stated purposes
- ◆ Aligned with statutory and contractual requirements (e.g., 8 years for PF records)
- ◆ Data securely deleted or anonymised upon expiry of retention period

6. DATA SECURITY

- ◆ Technical and organisational measures to protect data against unauthorized access, loss, or misuse
- ◆ Role-based access controls for HR systems
- ◆ Secure disposal of physical HR records

7. YOUR RIGHTS AS AN EMPLOYEE (DATA PRINCIPAL)

- ◆ **Access and correct** your personal data
- ◆ **Withdraw consent** where consent is the basis of processing
- ◆ **Raise grievances** regarding data processing

8. GRIEVANCE REDRESSAL

Grievance Officer	_____
Email	_____
Address	_____

This notice may be updated from time to time. Employees will be notified of material updates.

