PRIVACY AMBASSADOR IN ACTION

Department-Wise Implementation Guide

HUMAN RESOURCES DEPARTMENT

Custodians of Employee and Candidate Personal Data

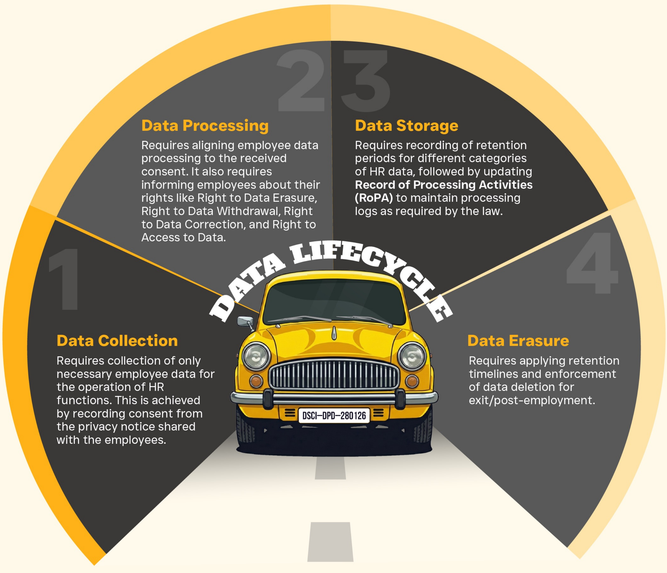
The HR Department is responsible for collecting, storing, and managing the personal information of employees throughout their employment.

According to the DPDP framework, they are required to ensure compliance with data protection laws by implementing secure handling practices, maintaining confidentiality, and enabling processing of HR data such as identity details, payroll information, and recruitment records.

DPDP FRAMEWORK APPLICATION AREAS

- Recruitment and Talent Acquisition
- Background Verification
- Employee Personal Data
- Insurance Administration
- Compensation and Payroll
- Performance Management and Appraisals
- Grievance & Disciplinary Records
- Exit Management

DATA LIFECYCLE



1 Data Collection

Requires collection of only necessary employee data for the operation of HR functions. This is achieved by recording consent from the privacy notice shared with the employees.

2 Data Processing

Requires aligning employee data processing to the received consent. It also requires informing employees about their rights like Right to Data Erasure, Right to Data Withdrawal, Right to Data Correction, and Right to Access to Data.

3 Data Storage

Requires recording of retention periods for different categories of HR data, followed by updating **Record of Processing Activities (RoPA)** to maintain processing logs as required by the law.

4 Data Erasure

Requires applying retention timelines and enforcement of data deletion for exit/post-employment.

KEY ACTIONS

- Review and update contracts with service providers for functions like payroll, insurance, background verification, recruitment, and benefits to ensure DPDP-compliant data processing obligations.
- Configure and set up HR Information Systems (HRIS) to record consent status.
- Maintain accessible grievance redressal channels for employees/candidates to raise data-related queries or complaints, with defined escalation paths to legal or compliance department.
- Align HR breach response procedures and employee communications with the organisation's overall personal data breach and incident response framework.
- Distinguish consent-based processing from legitimate employment-related processing.
- Conduct periodic training for HR personnel on DPDP obligations, grievance handling, data security practices, and employee data rights.

SUPPORTED BY

CRED · IIFL FINANCE · Kempegowda International Airport Bengaluru · PRIVASAPIEN · Protectt.ai · Providence · pnb · QRC · SQ1 n.rgen cybersecurity · target · ZS