



Job Description - Data Protection Officer (DPO)

Key Responsibilities -

Compliance Oversight

- Monitor the organization's end-to-end compliance with the DPDP Act 2023, including consent frameworks, data retention and erasure practices, data principal rights management, and cross-border transfer obligations
- Evaluate the existing data protection framework to identify gaps, areas of non-compliance, or partial compliance and recommend corrective actions
- Ensure that IT systems and processing procedures adhere to all applicable data privacy laws, RBI guidelines, and internal policies
- Maintain comprehensive data processing registers, records of processing activities (RoPA), and data flow maps

Data Protection Impact Assessments (DPIA)

- Identify high-risk processing activities requiring a DPIA and define the assessment methodology
- Review DPIAs for adequacy, advise on risk mitigation measures, and approve or recommend modifications to new projects, products, or services
- Ensure management formally responds to identified risks from DPIAs before processing commences

Grievance Redressal

- Act as the designated nodal officer for all grievance redressal as mandated under the DPDP Act
- Respond to complaints from Data Principals (customers, employees) within prescribed statutory timelines
- Ensure proper escalation procedures are followed and liaise with the Data Protection Board of India if grievances remain unresolved internally

Regulatory Liaison

- Serve as the **single point of contact** between the organization and the Data Protection Board of India
- Cooperate fully during audits, inspections, or investigations by the Data Protection Board
- Submit compliance reports and respond to regulatory queries in a timely and accurate manner
- Represent the organization in any proceedings before the Data Protection Board

Data Breach Management

- Establish, maintain, and test breach detection, assessment, containment, and notification procedures
- Ensure timely notification to the Data Protection Board and affected Data Principals in the event of a personal data breach
- Maintain an incident management plan and oversee timely remediation

Policy & Framework Development

- Develop, implement, and regularly update data protection policies, procedures, and internal frameworks
- Guide the organization in creating a detailed inventory (data map) of all personal data processing activities



- Ensure **Privacy by Design and Privacy by Default** principles are embedded in all new products, services, systems, and digital channels
- Oversee third-party processor compliance through vendor audits, contract reviews, and due diligence

Training & Awareness

- Design and conduct regular data protection training programs, staff seminars, and awareness campaigns for all employees involved in data processing
- Independently coordinate with departmental heads to build an organization-wide culture of data privacy
- Provide targeted awareness sessions for senior management and the Board on emerging privacy risks

Board Reporting

- Report **quarterly** (or as required) to the Board/Board Data Protection Committee on the organization's compliance posture, risk landscape, DPIAs completed, grievances resolved, and emerging threats
- Advise on data protection implications of strategic business decisions, mergers, acquisitions, or new product launches

Skillset - CISA/ CISM, CDPSE, IT Law, Risk, Regulatory Compliance, Regulatory Knowledge, Analytical Thinking

Qualifications - Bachelor's/Master's degree in Law , IT, Cyber Security, Compliance, or related field, LLB/LLM, B. Tech/MCA, MBA (Risk/Compliance), (Preferred)

Relevant Certifications - CIPP / CIPM, ISO 27701, CISA / CISM, CDPSE, ISO 27701 Lead Implementer / Auditor

Experience -

- Minimum 5–7 years of experience in data protection, privacy law, information security, legal compliance, or regulatory affairs
- Prior experience in the BFSI sector or with RBI-regulated entities is strongly preferred
- Demonstrated experience managing data breaches and regulatory investigations
- Monitor and advise on compliance with the DPDP Act, 2023, and internal privacy governance requirements across business functions
- Oversee implementation and periodic review of privacy policies, notices, consent mechanisms, retention practices, and erasure controls
- Act as the designated point of contact for Data Principals for grievance redressal and ensure complaints are addressed within applicable timelines
- Serve as the primary liaison with the Data Protection Board of India and support responses to audits, investigations, notices, and regulatory queries
- Guide business and technology teams on privacy-by-design measures for new products, services, systems, and processing activities
- Supervise or coordinate Data Protection Impact Assessments for high-risk processing activities and recommend risk mitigation measures
- Review data flows, records, and third-party processing arrangements to strengthen compliance and accountability
- Support incident response and verify that personal data breach detection, escalation, assessment, and notification processes are operational
- Deliver privacy awareness sessions and training programs for employees, contractors, and relevant stakeholders



- Prepare reports and dashboards for senior management and the Board on privacy risks, compliance status, grievances, and remediation progress

Location – Dombivli (Central Office)