

## **Data Protection Officer (DPO)**

### **Job Responsibilities:**

Data Protection Officer (DPO) shall act as the central authority for the implementation, oversight, monitoring, and enforcement of the Bank's Digital Personal Data Protection Program, in compliance with the Digital Personal Data Protection (DPDP) Act, 2023, RBI guidelines, and other applicable laws. The DPO shall independently advise the Bank, ensure accountability, protect the rights of Data Principals, and serve as the single point of contact with regulators, including the Data Protection Board of India.

Where required, the DPO may also act as the Grievance Officer under the DPDP Act.

### **Reporting Structure**

Reports functionally to: Board / Board Committee / Managing Director / Jt. Managing Director

Administrative reporting to: Senior Management

Operates independently without conflict of interest

### **Key Roles and Responsibilities: -**

#### **1. Policy, Governance & Compliance**

- A. Ensure the Bank's compliance with:
  - Digital Personal Data Protection Act, 2023
  - RBI, NABARD, and other applicable regulatory guidelines
- B. Develop, implement, review, and periodically update:
  - Digital Personal Data Protection Policy
  - Privacy Notices, Consent Frameworks, SOPs, and Standards
- C. Establish and maintain a Data Protection Governance Framework, including roles, responsibilities, and accountability across the Bank.
- D. Ensure privacy-by-design and privacy-by-default principles are embedded into business processes and IT systems.
- E. Monitor regulatory changes and assess their impact on Bank policies, processes, and systems.

#### **2. Risk Management & Assessments**

- A. Design and oversee the Data Protection Impact Assessment (DPIA) framework.
- B. Identify processing activities requiring DPIA and:
  - Review, approve, and monitor DPIA outcomes
  - Recommend risk mitigation measures
- C. Conduct and oversee privacy risk assessments for new products, services, systems, vendors, and process changes.
- D. Ensure maintenance and accuracy of:
  - Records of Processing Activities (RoPA)
  - Data flow maps and data inventories

#### **3. Data Principal Rights & Grievance Handling**

- A. Act as the single point of contact for Data Principals regarding:
  - Access, correction, erasure, consent withdrawal, and grievance redressal

- B. Establish and monitor procedures for:
  - Timely handling of Data Subject Access Requests (DSARs)
  - Resolution of privacy complaints and grievances
- C. Coordinate grievance redressal and escalation as per DPDP Act timelines.

#### **4. Incident & Breach Management**

- A. Define and oversee procedures for personal data breach management.
- B. Coordinate with IT, SOC, Legal, and Risk teams for:
  - Identification, containment, and remediation of breaches
- C. Ensure timely notification to:
  - Data Principals
  - Data Protection Board of India
  - Other regulators, as applicable
- D. Oversee root cause analysis and corrective action tracking.

#### **5. Third-Party & Cross-Border Data Governance**

- A. Oversee data protection controls related to:
  - Vendors, service providers, and outsourcing partners
- B. Ensure appropriate contractual safeguards, including:
  - Data protection clauses
  - Confidentiality and breach notification obligations
- C. Provide guidance on cross-border data transfers, including consent and contractual requirements.
- D. Ensure SLAs with third parties adequately address data protection obligations.

#### **6. Implementation, Monitoring & Audit**

- A. Oversee the Bank's Data Protection Office and coordinate with business, IT, Risk, Legal, HR, and Operations teams.
- B. Conduct or facilitate:
  - Periodic data protection audits
  - Compliance reviews of systems, manual records, backups, and archives
- C. Track remediation of audit findings and compliance gaps.
- D. Ensure appropriate data protection tools, controls, and technologies are in place.

#### **7. Awareness, Training & Culture**

- A. Design and deliver privacy awareness and training programs for employees and relevant stakeholders.
- B. Provide ongoing advisory support to staff on data protection issues.
- C. Define and monitor privacy-related KPIs for relevant roles and privacy champions.
- D. Promote a strong culture of data protection and accountability across the Bank.

#### **8. Regulatory & External Coordination**

- A. Serve as the primary liaison with:
  - Data Protection Board of India
  - Regulators, government bodies, and auditors
- B. Manage regulatory communications, reporting, and inspections related to data protection.
- C. Represent the Bank in matters related to data protection enforcement or regulatory actions.

### **Education & Qualifications**

- Graduation in Law, Information Security, Computer Science, IT, or related discipline
- Relevant certifications preferred:

- Data protection certificate
- Certified Data Professional (CDP)
- CIPP/E, CIPP/A, CIPM, CIPT
- CISM / CISSP
- ISO/IEC 27001 (Lead Implementer/Auditor)

## **Experience**

- 10–12+ years of experience in data protection, privacy, compliance, risk management, or information security
- Proven experience in:
  - Implementing privacy programs
  - Managing regulatory compliance and audits
  - Handling data breaches and DPIAs
- Banking / financial services experience is strongly preferred

## **Skills & Competencies**

- Strong knowledge of:
  - DPDP Act, 2023 and global privacy principles
- Ability to balance legal, technical, and business requirements
- Knowledge of Data Protection Act
- Understanding of IT and Data Processing
- Excellent stakeholder management and communication skills
- Demonstrated independence, integrity, and leadership
- Familiarity with privacy tools, risk management frameworks, and compliance monitoring systems

## **Authority & Independence**

- The DPO shall act independently and shall not receive instructions regarding the exercise of statutory duties.
- The Bank shall ensure adequate resources, authority, and access to information for effective discharge of responsibilities.