REQUEST FOR PROPOSAL (RFP)

Engagement of Consultant for the Implementation of Digital Personal Data Protection (DPDP) Act, 2023 Compliance Framework

Date of Issue of RFP: **March 16, 2026**

Last Date for Proposal: **April 10, 2026**

Preface

Dhanlaxmi Bank Ltd. (hereinafter referred to as "the Bank") invites proposals from eligible and reputed consulting firms for engagement as an implementation partner for operationalising compliance with the Digital Personal Data Protection Act, 2023 ("DPDP Act") and the Rules framed thereunder (collectively referred to as "DPDP Framework").

The Bank has already completed a comprehensive Gap Assessment against the requirements of the DPDP Act through an external consultant. Based on the identified gaps and the remediation roadmap, the Bank now intends to undertake a structured implementation programme to establish a robust, sustainable enterprise-wide privacy governance and data protection framework.

Accordingly, this Request for Proposal (RFP) is strictly for the implementation and operationalisation of the DPDP compliance framework. It shall not include fresh gap assessment activities, except for limited validation required for implementation planning.

The selected Consultant shall assist the Bank in implementing the remediation measures, strengthening privacy governance, embedding privacy-by-design principles across business processes and technology systems, and establishing sustainable mechanisms for ongoing compliance monitoring.

The Bank expects the engagement to result in a demonstrable, regulator-ready privacy framework aligned with the DPDP Act, applicable Rules, and relevant regulatory expectations applicable to scheduled commercial banks in India.

About Dhanlaxmi Bank Ltd.

Dhanlaxmi Bank Ltd. was incorporated in 1927 at Thrissur, Kerala, by a group of ambitious and enterprising entrepreneurs. Over the years, Dhanlaxmi Bank has earned the trust and goodwill of its customers through its strong commitment to relationship banking. It is due to our strong belief in the need to seek innovation, deliver the best service and demonstrate responsibility that we have grown from strength to strength. Be it in the number of customers, the scale of business, the breadth of our product offerings, the banking experience we offer or the trust that people invest in us. With 545 touch points (including 261 Branches, 284 ATMs) across India at your service, our focus has always been on customising services and personalising relations

Disclaimer

The information contained in this RFP document or information provided subsequently to applicants or consultants, whether verbally or in documentary form by or on behalf of Dhanlaxmi Bank, is provided to the bidder(s) or applicants on the terms and conditions set out in this RFP document and all other terms and conditions subject to which such information is provided. This RFP is neither an agreement nor an offer by the bank and does not claim to contain all the information each bidder or applicant may require. Each bidder or applicant may

conduct their own independent investigation and analysis and is free to verify the accuracy, reliability, and completeness of the information in this RFP. Bank may, in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP.

Confidentiality

This RFP is a confidential document and is not to be reproduced, transmitted, or made available by the recipient to any other entity without the Bank's express written permission.

RFP Schedule

The tentative schedule for the RFP process is as follows. The Bank reserves the right to modify the schedule at its discretion.

Activity	Date
Issue of RFP	16.03.2026
Last date for submission of queries/clarification	19.03.2026
Response to queries by the Bank	25.03.2026
Last date for submission of proposals	10.04.2026
Presentation/interaction with shortlisted bidders (if required)	20.04.2026

Submission and Evaluation of Proposals

The documents to be submitted are:

- Covering Letter
- Profile of the Consultant Firm
- Detailed technical proposal outlining implementation methodology
- Project plan with timelines
- Team structure and credentials
- Commercial proposal (separately submitted)

The proposals shall be submitted duly signed by the authorised signatory with the seal of the firm to the email address below, with the title:

"RFP for Engagement of Consultant for Implementation of Digital Personal Data Protection (DPDP) Act, 2023"

remya.joy@dhanbank.co.in

The bid evaluation will be processed using Least Cost Based Selection (LCBS) / Quality & Cost Based Selection (QCBS) as decided by the Bank.

For any clarifications regarding RFP, please contact:

Remya Joy
Data Protection Officer -In Charge
Dhanlaxmi Bank
Corporate Office, Thrissur
Email: remya.joy@dhanbank.co.in
Mobile:9539003634
Landline:0487 7107301

Objective of the Engagement

Implementation and Sustenance Support for Compliance with the Digital Personal Data Protection Act, 2023 (DPDP Act)

The Bank seeks to engage a qualified and experienced consulting partner to design, implement, and operationalise a comprehensive data privacy governance framework aligned with the requirements of the Digital Personal Data Protection Act, 2023 and applicable Rules.

The engagement shall include, but not be limited to:

- Validation of the Bank's existing DPDP Gap Assessment findings.
- Implementation of the remediation roadmap identified through the Gap Assessment.
- Establishment of a formal enterprise-wide privacy governance structure anchored by the Data Protection Officer (DPO) function.
- Operationalisation of data protection controls across systems, business processes, customer journeys, and third-party ecosystems.
- Development and implementation of privacy policies, procedures, and operational frameworks necessary for compliance with DPDP obligations.
- Enablement of appropriate technology tools and privacy automation capabilities, wherever required.
- Establishment of monitoring, reporting, and governance mechanisms to ensure sustained compliance with the DPDP framework.

The engagement is expected to ensure that the Bank achieves sustainable, auditable, and regulator-ready compliance with the DPDP Act**,** while embedding privacy considerations into the Bank's operational, technological, and governance processes.

Scope of Work

The selected Consultant shall assist the Bank in implementing the remediation roadmap identified through the DPDP Gap Assessment and in establishing a sustainable enterprise-wide privacy governance and compliance framework aligned with the Digital Personal Data Protection Act, 2023, and the Rules framed thereunder. The engagement is expected to focus on the design of the data protection governance framework, implementation of policies and processes, preparation of documentation, and advisory support for technology enablement

required for DPDP compliance. Development or deployment of new software solutions is not within the scope of this engagement unless specifically required and agreed upon by the Bank.

The implementation program shall be executed through the following phases:

Phase 1 – Discovery and Validation
Phase 2 – Privacy Governance and Framework Design
Phase 3 – Enterprise Privacy Implementation
Phase 4 – Compliance Testing and Validation
Phase 5 – Operationalisation and Training
Phase 6 – Sustenance and Continuous Compliance Support

1. Phase 1 – Discovery and Validation

The Consultant shall review and validate the Bank's existing DPDP Gap Assessment and confirm the scope of implementation.

Activities

- ✓ Review of the existing Gap Assessment report and remediation roadmap
- ✓ Validation of previously identified high-risk gaps
- ✓ Identification of additional gaps arising due to changes in systems, processes, products, or vendor ecosystem
- ✓ Validation of personal data inventory and data flow diagrams across business functions
- ✓ Identification of critical personal data processing activities within the Bank's operations
- ✓ Validation of third-party processors handling personal data
- ✓ Identification of cross-border personal data transfers within the Bank's ecosystem

Deliverables

- ✓ Validated Gap Register
- ✓ Updated Risk Heat Map
- ✓ Implementation Roadmap with prioritised remediation plan
- ✓ DPDP Compliance Control Matrix mapped to relevant provisions of the DPDP Act and applicable Rules

2. Phase 2 – Privacy Governance and Framework Design

The Consultant shall design and establish the Bank's enterprise privacy governance framework.

Activities

- ✓ Designing the operating model for the Data Protection Officer (DPO) Office
- ✓ Defining roles and responsibilities of relevant departments, including Compliance, Risk, Legal, IT, Cyber Security, Operations, Business Units and Vendor Management
- ✓ Establishing a Privacy Governance Committee and governance reporting framework
- ✓ Identifying and onboarding Department-level Privacy Champions

- ✓ Designing a data lifecycle governance framework covering collection, storage, usage, sharing and deletion of personal data
- ✓ Developing a data lifecycle RACI matrix

Policy and Framework Development

The Consultant shall review, develop, update and operationalise the following policy framework:

- ✓ Data Protection Policy
- ✓ Privacy Notice and Communication Policy
- ✓ Consent Management Policy
- ✓ Data Principal Rights Management Procedure
- ✓ Grievance Redressal Procedure
- ✓ Data Retention and Deletion Policy
- ✓ Third-Party Data Protection Policy
- ✓ Personal Data Breach Management Procedure
- ✓ Data Protection Impact Assessment (DPIA) Framework
- ✓ Enterprise-wide Records of Processing Activities (RoPA) Framework

Deliverables

- ✓ DPO Office Charter
- ✓ Privacy Governance Charter
- ✓ Privacy Policy Suite
- ✓ Privacy-by-Design Checklist
- ✓ DPIA Templates and Operating Procedures
- ✓ RoPA Framework
- ✓ Data Lifecycle Governance Framework

3. Phase 3 – Enterprise Privacy Implementation

The Consultant shall assist the Bank in implementing privacy controls across systems, processes, and customer journeys.

3.1 Customer Privacy Notice Framework

Activities

- ✓ Designing layered privacy notices across all customer interaction channels
- ✓ Standardising privacy notices for the Bank's website, mobile banking, internet banking, branch documentation, onboarding forms and customer communications
- ✓ Designing just-in-time disclosures across digital journeys

- ✓ Establishing notice change-control mechanisms

Deliverables

- ✓ Channel-wise privacy notice templates
- ✓ Notice approval and version control framework

3.2 Consent Management Framework

Activities

- ✓ Mapping consent capture points across all customer journeys
- ✓ Designing mechanisms for consent capture, modification, withdrawal and auditability
- ✓ Establishing consent propagation mechanisms across downstream systems
- ✓ Implementing cookie consent management across digital platforms
- ✓ Designing consent processes for minors and persons with disabilities, where applicable

Deliverables

- ✓ Enterprise Consent Management Framework
- ✓ Consent Lifecycle SOP
- ✓ Cookie Inventory and categorisation
- ✓ Consent Withdrawal and Audit Mechanism

3.3 Data Processing Controls & Security Safeguards

The Consultant shall assist the Bank in implementing privacy-aligned technical and operational controls.

Activities

- ✓ Implementation of data minimisation and purpose limitation controls
- ✓ Integration of Privacy-by-design integration in the product development lifecycle
- ✓ Review and strengthening of technical and organisational security safeguards, including:
  - Encryption
  - Access controls
  - Privileged access management
  - Secure APIs
  - Monitoring and audit logs
- ✓ Alignment with relevant RBI cybersecurity and IT governance guidelines

Deliverables

- ✓ Data minimisation framework
- ✓ Security safeguards assessment
- ✓ Privacy control implementation guidance
- ✓ Logging and monitoring standards

3.4 Third-Party Privacy Risk Management

The Consultant shall establish a privacy-focused Third-Party Risk Management (TPRM) framework.

This shall cover:

- ✓ Business Correspondents
- ✓ Direct Selling Agents
- ✓ Card processors and networks
- ✓ Payment gateways
- ✓ IT & Non-IT vendors and service providers
- ✓ Analytics and marketing partners

Activities

- ✓ Identification of third-party data processors, including vendors, fintech partners, Business Correspondents, DSAs, card networks and service providers
- ✓ Development of a third-party privacy risk classification framework
- ✓ Updating vendor onboarding due diligence processes
- ✓ Drafting DPDP-aligned contractual clauses for vendor agreements
- ✓ Establishing vendor monitoring mechanisms

Deliverables

- ✓ Third-Party Data Processor Register
- ✓ Vendor Privacy Risk Assessment Framework
- ✓ DPDP-aligned contractual clauses
- ✓ Third-party monitoring mechanism

3.5 Data Retention, Erasure & Deletion Controls

The Consultant shall assist the Bank in implementing end-to-end data lifecycle management controls.

Activities

- ✓ Reviewing existing data retention schedules
- ✓ Alignment of retention requirements with regulatory obligations
- ✓ Designing data deletion and erasure mechanisms across:
  - o Core banking systems

- Data lakes
- Document management systems
- Backups and disaster recovery environments
- Third-party processors, etc

Deliverables

- ✓ Updated Data Retention Schedule
- ✓ Data Deletion & Erasure SOP
- ✓ Deletion evidence and reconciliation framework

3.6 Data Principal Rights & Grievance Management

The Consultant shall implement an operational framework for managing Data Principal rights requests.

Activities

- ✓ Designing intake channels for Data Principal rights requests
- ✓ Establishing identity verification mechanisms for request processing
- ✓ Integration of rights request processing into customer service workflows
- ✓ Establishing SLAs and escalation procedures for grievance redressal

Deliverables

- ✓ Data Principal Rights SOP
- ✓ Rights request processing workflow
- ✓ Customer Response Templates
- ✓ Rights & Grievance Tracking Mechanism

3.7 Personal Data Breach Management

The Consultant shall develop and operationalise a personal data breach management framework.

Activities

- ✓ Integration of privacy breach management with the Bank's incident management framework
- ✓ Development of breach detection, escalation and reporting procedures
- ✓ Designing breach notification workflows
- ✓ Conducting breach simulation exercises

Deliverables

- ✓ Personal Data Breach Management SOP
- ✓ Breach Escalation Matrix
- ✓ Incident Response Playbook

3.8 Cross-Border Data Transfer Governance

The Consultant shall identify and assess all cross-border transfers of personal data within the Bank's ecosystem.

Activities

- ✓ Identification of cross-border personal data transfers
- ✓ Classification of cross-border data flows
- ✓ Assessment of legal permissibility under DPDP provisions
- ✓ Development of contractual and operational safeguards

Deliverables

- ✓ Cross-Border Data Transfer Register
- ✓ Transfer approval framework
- ✓ Processor contractual safeguards

3.9 Privacy Technology Enablement

The Consultant shall support the Bank in evaluating and implementing privacy technology solutions where required.

Areas may include:

- ✓ Consent management tools
- ✓ Data discovery and mapping tools
- ✓ Data subject request management tools
- ✓ DPIA automation tools
- ✓ Vendor privacy risk management tools

Deliverables

- ✓ Privacy Technology Evaluation Report
- ✓ Technology Implementation Roadmap
- ✓ User Acceptance Testing (UAT) Support Documentation

4. Phase 4 – Compliance Testing and Validation

The Consultant shall conduct testing and validation of the implemented privacy controls.

Activities

- ✓ Privacy control testing
- ✓ DPIA validation exercises
- ✓ Breach readiness assessment
- ✓ Compliance validation against DPDP requirements

Deliverables

- ✓ Privacy Compliance Validation Report
- ✓ Residual Risk Register

5. Phase 5 – Operationalisation and Training

Activities

- ✓ Development of operational procedures for the DPO office
- ✓ Training programs for privacy champions and relevant departments
- ✓ Conducting Bank-wide privacy awareness programs

Deliverables

- ✓ Privacy Training Materials
- ✓ Operational SOPs
- ✓ Privacy Awareness Program Reports

6. Phase 6 – Sustenance and Continuous Compliance Support

Activities

- ✓ Establishing privacy KPIs and monitoring dashboards
- ✓ Conducting periodic privacy compliance reviews
- ✓ Monitoring third-party privacy risks
- ✓ Updating policies based on regulatory changes

Deliverables

- ✓ Privacy KPI Dashboard
- ✓ Annual Privacy Compliance Review
- ✓ Updated Policy Documentation
- ✓ Privacy Governance Reporting Framework

Expected Outcome

Upon completion of the engagement, the Bank shall have:

• A fully operational DPDP compliance framework
• A formal enterprise privacy governance structure
• Implemented privacy controls across systems and processes
• Integrated third-party privacy risk management
• Sustainable privacy monitoring and compliance mechanisms embedded into business operations.

Regulatory Alignment Requirement

During the contract period, the Consultant shall incorporate any new regulatory requirements, guidance, or notifications issued under the Digital Personal Data Protection Act, 2023 and associated Rules into the Bank's implementation framework without additional cost, provided such changes fall within the scope of this engagement.

Indicative Milestones and Deliverables

The implementation program is expected to be executed through the phases outlined in this RFP. The following table provides an indicative set of milestones and key deliverables expected from the Consultant. The detailed project plan, timelines, and activity sequencing shall be proposed by the selected Consultant and approved by the Bank.

Phase	Key Deliverables	Indicative Timeline
Phase 1 – Discovery and Validation	Validation of Gap Assessment, Updated Gap Register, Risk Heat Map, Implementation Roadmap	Month 1
Phase 2 – Privacy Governance and Framework Design	DPO Office Charter, Privacy Governance Framework, Policy Suite, RoPA Framework, DPIA Templates	Month 2 – 3
Phase 3 – Enterprise Privacy Implementation	Consent Framework, Privacy Notices, Data Retention Controls, Vendor Privacy Risk Framework, Breach Management Framework	Month 3 – 6
Phase 4 – Compliance Testing and Validation	Privacy Control Testing, Compliance Validation Report, Residual Risk Register	Month 6 – 7
Phase 5 – Operationalisation and Training	Privacy Training Programs, Operational SOPs, Privacy Champion Enablement	Month 7 – 8
Phase 6 – Sustenance and Continuous Compliance Support	Privacy KPI Dashboard, Monitoring Framework, Periodic Compliance Reviews	Month 9 onwards

Evaluation of Proposals

The Bank will evaluate proposals received in response to this RFP based on technical and commercial considerations, including but not limited to the bidder's relevant experience, understanding of the assignment, proposed methodology, team composition, and commercial proposal.

The Bank may adopt such an evaluation methodology as it considers appropriate for selecting the Consultant. The Bank reserves the right to seek clarifications, conduct presentations or interactions with shortlisted bidders, and to modify the evaluation process where necessary.

The Bank's decision on the evaluation of proposals and the selection of the Consultant shall be final and binding.

Eligibility Criteria

Bidders must meet the following eligibility criteria to participate in the RFP process. The Bank reserves the right to verify the information submitted by bidders and to seek additional supporting documents where necessary.

1. Legal Status of the Firm

The bidder must be a company or limited liability partnership incorporated in India under the applicable laws (Companies Act / LLP Act). The firm must have been in operation for a minimum of five (5) years as of the date of submission of the proposal.

2. Relevant Experience

The bidder should have demonstrable experience in implementing data privacy or data protection regulatory frameworks.

The bidder must have completed at least:

• Two (2) assignments relating to the implementation or advisory of data privacy/data protection regulations (such as DPDP Act, GDPR, or equivalent privacy regulations), and
• At least one (1) such assignment in a scheduled commercial bank, financial institution, NBFC, insurance company, or other regulated financial sector entity in India.

3. Banking / Financial Sector Experience

The bidder should possess an adequate understanding of the regulatory and operational environment of banks and financial institutions in India, including handling of customer personal data across core banking systems, digital banking channels, and third-party ecosystems.

4. Professional Expertise

The bidder must deploy a team with appropriate expertise in data privacy governance, regulatory compliance, and technology implementation. The proposed team should include professionals with relevant experience in implementing privacy regulations and data protection governance.

Preference may be given to bidders with professionals holding internationally recognised privacy certifications, such as Certified Information Privacy Professional (CIPP), Certified Information Privacy Manager (CIPM), or equivalent qualifications.

5. Technical Capability

The bidder should be able to support the implementation of privacy frameworks across business processes, technology systems, and third-party ecosystems. The bidder should also be able to evaluate and support the implementation of privacy technology tools where required.

6. Financial Stability

The bidder should have a stable financial position and should not have been declared insolvent or bankrupt. The firm should not have been blocked or debarred by any government authority, regulatory body, or financial institution in India.

7. Conflict of Interest

The bidder must disclose any potential conflict of interest that may arise in connection with this engagement. The Bank reserves the right to reject proposals where a conflict of interest is identified.

8. Compliance with Laws

The bidder must comply with all applicable laws and regulations in India and must not be involved in any ongoing legal proceedings that may materially affect its ability to undertake the assignment.

General Terms & Conditions

- All the software and hardware equipment, like laptops, tools, etc., to carry out the assignment have to be brought by the consultants at no extra cost.

- The consultant shall provide a letter of intent acknowledging the terms of the RFP document.

- The contract with the consultant shall be governed in accordance with the laws of India for the time being in force and will be subject to the exclusive jurisdiction of the courts of Thrissur, Kerala.

- The bank is not bound to give reasons for declining any or all of the proposals

- The bank is not bound to accept the lowest or any bid and may cancel the bidding process at any stage before the award of the contract, and is not bound to provide reasons for cancellation.

- Bank reserves the right to modify the scope due to a change in regulatory instructions and internal requirements within the overall objective of consultancy services during the course of the project. There might be related areas that the bank would like the selected bidder/consultant to undertake that were not envisaged earlier. Bank shall also reserve the right to change the timelines to comply with regulatory guidelines without any additional cost.

- Any extension/ modification of the completion date due to unforeseen delays may be permissible by the bank at its sole discretion. However, no additional amounts shall be payable by the bank towards completion of the assignment beyond the implementation periods specified in the scope.

- Proposal should be valid for at least 90 days after the closing date, and prices shall be locked for the entire contract period.

- The assessment process shall be commenced within a week from the date of acceptance of the purchase order.

- The terms of payment shall be mutually discussed and agreed upon before issuing the PO. All out-of-pocket expenses, travelling, boarding, lodging and other expenses, if any, to be incurred by the consultant shall be included in the bid submitted by the consultant, and no extra cost thereof shall be payable by the bank for the same.

- Completion of the process is ----- months from the date of commencement of the assessment.

- Bank reserves the right to modify the scope in line with regulatory changes.

- The Bank reserves the right to accept or reject any proposal, or to cancel the RFP process at any stage without assigning any reason.

Bidder's Particulars

Sl.no.	Particulars	To be furnished by the bidder
1.	Name of the firm	
2.	Address of the firm	
3.	GST number of the firm PAN number of the firm	
4.	Particulars of the Primary contact Official |Name |Designation |Address |Mobile |Landline |Email	
5.	Details of other assignments by the firm or its associates with Dhanlaxmi Bank	
6.	Experience of the firm in handling a similar assignment of gap assessment against DPDPA	
7.	Cost for end-to-end implementation of DPDP compliance as detailed in the RFP.	

With reference to the above RFP, having examined and understood the instructions, terms and conditions forming part of the RFP, we hereby enclose our offer for providing said solution as detailed in your above-referred RFP.

We confirm that the offer complies with the terms and conditions set out in the above-cited tender and agree to all the terms and conditions of the RFP and any subsequent amendments. We confirm that we agree to all the terms and conditions set out in this RFP.

Authorized Signatory
Name and Designation Office Seal

Place :
Date :