SECTION-E: REVISED SCOPE OF WORK

1. General

The scope of work includes end-to-end implementation and support covering all aspects of the DPDP Act & Rules, as detailed in this RFP and its Annexures. The Consultant shall undertake applicability and gap assessments; design and implement the DPDP governance framework; develop guidelines, policies, SOPs, templates, data flow diagrams, risk categorization matrices, and DPIAs; and provide project management consultancy support for floating and evaluating RFPs for procurement of privacy automation tools.

The Scope of Work (SoW) under this RFP is intentionally structured in a modular, activity-wise manner. LIC reserves the absolute, unconditional, and irrevocable right, at any stage of the engagement, to:

a) Exclude, defer, modify, or independently execute any activity, sub-activity, or work stream defined in the SoW, including but not limited to technology procurement, RFP preparation, vendor evaluation, and implementation support for any DPDP-related tool or platform; and

b) Assign or engage any other vendor(s) or internal teams to carry out such excluded or modified activities, without any financial, contractual, operational, or delivery impact on the balance Scope of Work.

In such circumstances, the Consultant shall be entitled only to payment for those activities actually performed and formally accepted by LIC. The commercial value attributable to the excluded or de-scoped activities shall be proportionately deducted from the total contract value, and the Consultant shall have no claim whatsoever for compensation, loss of opportunity, idle resources, overheads, or anticipated profits.

The Bidder shall submit its commercial proposal with clear, unbundled, and activity-wise pricing, mapped on a one-to-one basis with the Scope of Work. LIC reserves the right to accept, reject, modify, or de-scope any activity, in full or in part, and the corresponding commercial value shall stand reduced accordingly.

This scope is indicative and not exhaustive. The Bidder is expected to absorb any other cost of material / services if any not particularly listed below.

1.1. Objectives of the Engagement

The objective of this engagement is to undertake an enterprise-wide DPDP compliance program covering assessment, design, implementation, technology enablement, training, governance, and ongoing compliance assurance. The Consultant shall enable LIC to meet its obligations as a Data Fiduciary, Significant Data Fiduciary and Data processor in a structured, auditable, and sustainable manner.

1.2 Scope Coverage

The Scope shall cover all personal data processed by LIC in any form (digital, physical and digitized personal data), including data relating to policyholders, prospects, nominees, employees (on-roll and off-roll), pensioners, agents, intermediaries, vendors, contractors, website visitors and mobile application users, digital journey users etc.

Coverage shall extend across all environments and operational locations, including Central Office, Zonal Offices, Divisional Offices, Branch Offices, Satellite Offices, Mini offices, 8 Data Centers (located at Mumbai, Navi Mumbai, Bangalore, Hyderabad, Bhubaneswar, Noida), Disaster Recovery (DR) sites, Cloud environments, third-party platforms etc. This includes COLOs, ZTCs, ATCs, MDC, Premium Points, Agents, Development Officers, cross-border data and offices, as well as UAT/Test environments, encompassing Backup and DR systems and Logs and Monitoring infrastructure.

The assessment shall cover all departments and their respective sections within LIC, (indicative number 35). The indicative number of applications proposed to be covered under the assessment is 300.

LIC offers five broad categories of products, each comprising multiple sub-products. At present, 60 products are active, while approximately 250 products have been withdrawn over the years, for which servicing is still being provided.

1.3. Applicability Assessment & Comprehensive Gap Assessment (Foundational Phase)

The Consultant shall conduct a comprehensive, enterprise-wide Privacy Impact and Gap Assessment at the commencement of the engagement. The findings from this phase shall concurrently guide and support activities undertaken in other phases.

The Gap Assessment shall include:

A. Legal & Regulatory Gap Assessment

- Mapping of DPDP Act Sections 4–16 and DPDP Rules against existing LIC policies, procedures and practices.
- Identification of non-compliance, partial compliance and over-compliance areas
- Identification of potential penalties, legal exposure and reputational risks
- Identify and enlist the legal implications and financial penalties that may be attracted if LIC fails to adhere to the stipulated data protection measures.

B. Business Process & Operational Gap Assessment

- Study & Understand comprehensively the provisions & requirements of DPDPA and any subsequent amendments/updates. Identify the list of products and services offered by LIC and Assess applicability of provisions of the DPDP Act on it
- Review of all core insurance processes, including but not limited to, onboarding, underwriting, Marketing, policy administration, claims, servicing etc.
- Review of support functions, including but not limited to, HR, IT, Finance, Payroll, Legal, Procurement, Actuarial etc.
- Identification of lawful basis for processing under act ("consent vs legitimate use")
- Assessment of consent, notice, purpose limitation, data minimization, retention and erasure.
- Study existing roles, responsibilities and reporting structures covering all the stakeholders, entire organization.
- Detailed assessment of product, product life cycle, data infrastructure, Cross-selling & sharing of data and its risk assessment.
- Assessment of secondary uses such as but not limited to, data enrichment, analytics, profiling, Upselling, cross selling & marketing reuse of personal data beyond the originality.

C. Privacy Impact Assessment (PIA)

- Ensure conformance with applicable legal, regulatory, and policy requirements for privacy;
- Determine the risks and effects; and.
- Evaluate protections and alternative processes to mitigate potential privacy risks.

D. Technology & Security Gap Assessment

- Evaluation of data security measures covering applications, databases, endpoints, networks and infrastructure for meeting the requirements as per the Act.
- Assessment of access control, encryption, logging, SOC, incident response, DLP and breach detection for meeting the requirements as per the Act
- Evaluate internal tools and processes for meeting the requirements as per the act.
- Evaluate the existing controls for meeting the requirements as per the Act.
- Assessment of backup system, disaster recovery environments, logs, test & UAT environment and usage of masked or non-masked personal data outside production system.
- Assessment of rationalization of Quantum of personal data processed and implementation of secure storage, retrieval and disposal mechanism in line with Data minimization principle of sensitive information .
- Highlight the risks identified during review of the personal data lifecycle
- DPIA of Applications dealing with personal data.
- The following shall not be a part of the bidders' scope. However the bidder may leverage the existing reports for the Security Gap Assessment
- Source code review
- Penetration testing
- Forensic log analysis
- Red-team / blue-team exercises

- CA and VA
- SNA review

E. Vendor & Third-Party Gap Assessment

- Conduct privacy risk assessment of vendors.
- Review of data, data sharing mechanism with agents, intermediaries, processors and outsourcing partners
- Review of contracts, data sharing clauses, indemnities and liabilities of agents, intermediaries, processors and outsourcing partners.
- Obtain a list of third party with whom personal data is shared for processing.
- Develop a control framework and audit checklist based on DPDP act to assess vendors' privacy posture. For effort estimation, the bidder may take 200 vendors into account.
- Identify all data processors & sharing partners.

F. Governance & Organizational Gap Assessment

- Review of DPO role, reporting structure, escalation mechanisms and KPIs.
- Assessment of Significant Data Fiduciary readiness as per the Act.
- Personal data governance- Assessment of personal data governance model including ownership & stewardship, decision making authority, escalation mechanisms and accountability structure etc.
- Consent Manager, Grievance Officer, Independent Data Auditor
- RACI and escalation matrix
- Identification of Data/process owners for each business functions for clear ownership of data.
- Design and implementation support for publication of DPO contact details, Grievance mechanism and escalation process on LIC websites, Mobile apps & customer facing Platform's as mandated under
- Provide Remediation for all Gaps Identified in points A-F.
- Deliverable: Applicability Assessment report, PIA Report, Detailed Gap Assessment Report with risk scoring and remediation roadmap and implementation of suggested remediation to be done by consultant.

1.4. Data Discovery & Mapping

- This phase shall identify and document LIC's personal data landscape.
- Study and understand comprehensively the provisions& requirements of Digital Personal Data Protection Act (DPDP) act /rules and any subsequent amendments/updates
- Identify & Assess All Data Touch Points in existing structure of LIC and associated third Party platforms for Data related functions like Data Entry, Exit, Process, Storage, Erasure, and other Data Handling activities/all types of Data Flows, either digital or physical data (later digitized) being handled in LIC/of LIC/for LIC.
- Understand exhaustively the existing Data Infrastructure which shall include to Identify and Assess comprehensively the tools, systems, software, applications, channels, and other technological Infra structure employed/ used in the entire data handling process/functions at all the points within LIC when Data is in transit, use and at rest (i.e. Data Entry, Exit, Storage, Processing, Sharing, Retention, Disposal, etc.) as part of extant data management infrastructure.
- Hybrid data discovery (automated and manual) and assessment of data storage locations, including but not limited to servers, endpoints, backup media, tapes, and other storage repositories. The Bidder shall provide all necessary tools, utilities, and resources required for this activity, with no dependency on LIC for tools, licenses, or infrastructure.
- Identification of structured, unstructured and physical data
- Creation of enterprise Personal Data Inventory and Data Dictionary
- AI/ML-powered scanning of structured and unstructured data.
- Identification of personal data across systems.
- Risk-based categorization and tagging.
- Identification of personal data, children and PwD data. Age verification mechanisms,

- Orchestrate data deletion requests with various internal stakeholders and the Data Processors. Enable processes to verify artefacts and related to the deletion request.
- Define processes to ensure that personal data resides only in the designated servers.
- Mapping of end-to-end data flows (collection → processing → storage → sharing → archival → erasure)
- Identification of cross-border data processing.
- Identification of Single Source of Truth opportunities
- Deliverable- Data Flow Diagrams (DFDs) including an Enterprise-wide Personal Data Inventory and Data Lineage. The Data Inventory shall be structured, accurate, and reusable for statutory and regulatory requirements, including ROPA, DPIA, and internal/external audits.

1.5. DPDP Framework & Policy Design

The Consultant shall design the DPDP compliance framework in parallel with the Gap Assessment, incorporating inputs and findings from the Gap Assessment on an ongoing basis.

1.5.1 Governance Framework

- Data Protection Officer (DPO) roles and responsibilities
- Consent Manager, Grievance Officer, Independent Data Auditor
- RACI and escalation matrix
- Mapping of Data/process owners for each business functions for clear ownership of data.
- Design and implementation support for publication of DPO contact details, Grievance mechanism and escalation process on LIC websites, Mobile apps & customer facing Platform's as mandated under DPDP Act.
- Any Other aspect mentioned under DPDP Act, which has not been stipulated above.

1.5.2 Policy, Templates & SOP Suite

- Data Privacy Policy
- Privacy Notice and Cookie Policy
- Consent Management Policy
- Data Retention and Erasure Policy as per the Act.
- Personal Data Breach Management Policy
- Third Party & Outsourcing Privacy Policy
- Cloud and AI Governance Framework
- Internal Data Sharing SOP and Mechanism.
- Data Governance Policy- covering secondary use of data, guidelines of data ownership cross border data sharing etc.
- Information Security & Cyber Policy
- Grievance Redressal Policy
- Data Subject Request Handling Guidelines
- Data Principal Rights Management Policy
- Cyber Crisis Management Policy
- Vendor Audit Reports and Assessment Framework

1.5.3 Notices, Consent & Legitimate Use

- Purpose-specific notices
- Mandatory vs optional consent mapping- Identifying and documenting which personal data processing activities require mandatory consent under the DPDP Act
- Legitimate use assessment- Evaluating whether personal data can be processed without consent under the "legitimate uses" permitted by the DPDP Act
- Controls to prevent secondary use of data without lawful basis as per DPDP Act
- Design of Multilingual privacy notices, Consent form and customer communication aligned with pan India customer base and regulatory communication requirements as per DPDP Act/rules.

- Design of consent collection, modification and withdrawal workflow.
- Design of Notice workflow

1.5.4 Data Principal Rights

- Design of Access, correction, updation, erasure, grievance, nomination workflows
- Nomination and Grievance Rights
- Verification and authentication of Data principals
- Timelines and escalation mechanism for rights fulfillment
- The Bidder shall be allowed to leverage the existing customer service or grievance platforms for the purpose.

1.5.5 DPIA Framework

A. Comprehensive DPIA Templates & Workflows

- Provide standardized templates and workflows for conducting DPIAs, covering:
  i. Description of processing activities, including involvement of third parties
  ii. Risk assessment matrix to evaluate risks and automated risk calculation & categorization of all products/ process wise.
  iii. Regulatory and industry specific DPIA templates, customizable as per business needs.
  iv. The expected frequency of DPIA should be as per the DPDP Act and Rules (Annually or if there are any changes in the intervening period)

1.6 Implementation & Technology Enablement

- The Consultant shall support the implementation and closure of all identified remediation actions.
- Design, enable, and operationalize tool based Automated Records of Processing Activities (ROPA).
- Implement and support automated data discovery and data classification tools.
- Ensure that DPDP Act–mandated controls are embedded into applications, systems, and business processes.
- The Bidder shall enable and support automation-driven controls to reduce compliance risk, improve accuracy, and ensure sustained regulatory compliance.
- Privacy-by-design support for new initiatives
- Assist in End to End implementation & Integration of the tools procured through Project Management Consultancy with LIC environment.

1.6.1 Project Management Consultancy-

- The bidder has to assist in preparation and evaluation of RFPs for on-boarding vendors for procurement of tools related to implementation of DPDP Act.
- The RFPs shall comprehensively cover modules including but not limited to, Consent Management Platform, Digital principal Rights Management, Grievance Redressal, Cookie Consent Management, DPIA tools, Data Privacy Notice Management, Data Breach Management, Compliance reporting & Dashboards, Workflow management, Data Discovery & Mapping, DPDP awareness and implementation portal.
- Provide technical evaluation support for RFP responses
- Ensure workflow automation and continuous DPDP compliance adherence
- Assist in End to End implementation & Integration of the above mentioned tools with LIC environment.
- Maintenance and sustenance of the implemented tools.
- Prior to the onboarding of vendor under the PMC projects the bidder should complete the following aspects from Sec 1.6.2 to 1.6.8. (Indicative list only)

1.6.2 Consent Management

- Design, implement, and operationalize an enterprise-wide consent management framework, including requisite policies, procedures, standards, templates, and technical controls, to be uniformly adopted across all products, applications, and internal business functions. The framework shall be fully compliant with the DPDP Act and applicable Rules, and shall support retrospective consent wherever required.
- The framework should be able to cater measures for collection, storage, modification, and withdrawal of consent as well as demonstrating recording of the said process.
- Framing appropriate model consent form (physical/digital) for different category of products/ processes/ purposes as per DPDPA.
- Identify the consent collection points across each product/business function and assist the various product owners to integrate DPDPA's consent requirements with in the irrespective consent journeys.
- Assist relevant teams in consent log management, tagging and effectively ensure that consent including its modification and revocation travels with the personal data element
- Develop business requirement document and assist LIC in evaluating vendors for implementing tools to manage consent.
- Actively suggest and participate in tool demos to help LIC to identify the best fit as per its processing needs.
- Identify and connect with various departments/business functions to determine and communicate their accountability and responsibility with respect to consent management.
- Analyze the impact of consent modification/revocation by Data Principals on processes/customer relationship management/business intelligence/marketing leads generation etc.
- Analyze cookie consent and preference management framework with a detailed cookie notice. Integrate the cookie consent across the data processing systems to ensure consensual processing of data collected through cookies.
- Dynamic notice generation capability with comprehensive and short notice for future regulatory changes with the help of Data Privacy Notice Management tool.

1.6.3 Data Principal Rights Management

- Create Data Principal Rights Management Process with inputs from relevant stakeholders. Assess existing setup for operationalization of this request and assist in new deployment. Understand personal data processing activities across each product/ process and type of personal data processed, in a way data principals can exercise their data privacy rights and raise their grievances.
- Develop Data Principal Rights Management process covering identity verification, recording, validation, and timely response to data principal request.
- Assist in establishing Data minimization and data limitation Principles
- Create a detailed RACI with all stakeholders to ensure tracking of accountability and responsibility of all stakeholders.
- Discuss with relevant stakeholders to obtain their input and signoff.
- Develop business requirement document and assist LIC in evaluating vendors for implementing tools to manage data principal rights.

1.6.4 Vendor/ Third party Contract

- Vendor contract remediation and standard contractual clauses of agents, intermediaries, processors and outsourcing partners.
- Retention and erasure of historical data taking into account the Act and applicable regulatory guidelines
- Vendor Data-Sharing Register and standardized DPDP-compliant contractual clauses/templates.

1.6.5 Data Breach Management

A. Regulatory Reporting & Compliance

- Breach reporting mechanism to be in place/facilitated.
- The workflow of breach investigation & intimation should align the requirement as per Rules of the DPDP Act. Seamless reporting to the Data Protection Board and Data Principals.
- Implement the mechanism to maintain a repository of pre-approved templates for quick and compliant breach reporting.
- Show steps taken to contain the breach, demonstrating transparency and trust.

B. Final Communication & Documentation

- Implement the mechanism to send initial and final breach reports to both impacted Data Principals and Data Protection Board
- Maintain an audit trail of all breach-related actions for demonstration of compliance.

C. Bulk Breach Notifications

- Create cohorts of Data Principals to ensure that the notification is only going out to the affected Data Principals.
- Configurable templates for breach intimation, ensuring compliance and clarity.

1.6.6 Grievance Redressal Mechanism

- Create grievance redressal process/workflow to meet the grievance redressal deadlines issued by the Act/Rules
- Connect with legal teams to templatize/frame responses and prevent any risks while responding to the grievances
- Create an RACI/escalation Matrix with oversight from Relevant departments

1.6.7 DPIA Tool

A. Design automated DPIA workflow with following indicative requirements but not limited to and integrate it with the DPIA tool procured through PMC -

i. Enable multi-level workflow capability to facilitate role-based access, permissions, and approvals.
ii. Allow customization of roles, permissions, and review processes to align with organizational structures.
iii. Support auto-reminders, query escalation, and follow-ups to streamline DPIA completion.
iv. Provide the ability to upload supporting documents and artifacts when responding to specific queries.
v. Periodic & Proactive Assessments
vi. Support periodic DPIA reviews to ensure ongoing compliance with regulatory requirements.
vii. Proactively launch assessments for new business processes, with a timeline view for accountability and visibility.

- Design automated vendor assessment workflow.
- Enable seamless sharing of DPIA assessments with data processors and vendors, ensuring end-to-end compliance.
- Provide functionality to add team members and external stakeholders for collaborative assessments.
- Auto-fill assessments using AI leveraging knowledge base of consent artifacts, processors, configurations and data discovery findings.
- Integrate DPIA with existing Audits to prevent any overlaps and gaps.

B. Controls, Reporting and Dashboard

- Real Time Monitoring: Dashboard should provide real time visibility into the initiation, review, approval and closure of DPIAs across all Branches and Business functions.

- SLA Based Time Tracking: The tool must include automated time tracking of each DPIA process step, with configurable Service Level Agreements (SLAs) and dynamic indicators (e.g. red/yellow/green flags) for SLA compliance.
- Alerts and Escalations: Support for automated alerts and escalations to DPOs, Privacy Stewards, or relevant functionaries in case of SLA breaches or pending approvals.
- Branch Wise & Function Wise Compliance Overview: Ability to generate compliance scorecards and dashboards for each branch, Division, Zone, Department or business Vertical.
- Role-Based Access Controls (RBAC): The system should allow differentiated access for
- DPO – Global access with configuration and oversight privileges
- Privacy Stewards – Access to DPIAs within their assigned Divisions/Zones/Functions/Verticals
- Branch/Division/Zone/Central Office – Access to DPIAs initiated or owned by their teams
- The platform must be scalable to onboard all branches and new privacy stakeholders as per future organizational requirements

1.6.8 Data Classification Tool

- The tool shall support compliance with the Digital Personal Data Protection Act, 2023 and DPDP Rules, 2025 by enabling identification, classification, and governance of Digital Personal Data (DPD) across the organization.
- Automatically discover and identify personal data (structured and unstructured) across databases, applications, file systems, endpoints, APIs, and cloud environments.
- Classify data based on sensitivity, risk, purpose of processing, and retention requirements, aligned with the organization's data classification policy and DPDP obligations.
- Support identification of high-risk personal data and enable risk-based tagging to facilitate DPIAs and enhanced safeguards.
- Support linkage of classified data with consent status and purpose limitation, and highlight deviations.

1.7 Operations, Training & Compliance Assurance

1.7.1 Training

- Organization-wide DPDP awareness and training which shall include all stakeholders of LIC such as bot not limited to employees, agents, intermediaries, vendors etc.
- LIC will discover the commercial for 200 training sessions and will conduct the trainings as per the actual requirements. Payment will be made on a pro-rate basis. Out of the 200 training sessions 100 may be ear marked for online and the remaining as offline.
- Role-based training and awareness programs
- Tabletop breach simulations exercise every quarter. Total 20 during the project period.
- Training materials

1.7.2 DPDP awareness and implementation portal

As part of the engagement, the Consultant shall design, configure, and operationalize a centralized DPDP Awareness and Self-Certification Portal to enable sustained compliance across Employees, Agents, Intermediaries, and other Authorized users handling personal data.

The portal shall support:

- Role-based DPDP awareness content aligned to the Digital Personal Data Protection Act, 2023 and DPDP Rules, 2025
- Periodic self-certification by users confirming understanding and adherence to DPDP obligations
- Mandatory acknowledgements of DPDP policies, notices, and acceptable data handling practices
- Online assessments with configurable pass/fail thresholds
- Multilingual support aligned to organizational and statutory requirements
- Audit-ready logs capturing training completion, certification status, timestamps, and user identity

- Management dashboards and MIS reports for compliance tracking and regulatory evidence
- The Portal should be deployed Onsite.

The Consultant shall ensure that the portal is scalable, secure, and capable of integration with existing identity, HRMS, agency management, or learning platforms, where applicable.

Only the Hardware (VMs), Network Infrastructure, JBoss Enterprise Application Server, RHEL OS, MySQL (if required), will be provisioned for this by LIC on own premise data center, rest all is to be provisioned by Consultant.

Ownership, administrative access, and all artefacts developed under this activity shall vest with LIC.

1.7.3 DPDP Program Management, Reporting, Collaboration and Evidence Management Portal

The Consultant shall **design, configure, and operationalize a centralized DPDP Program Management Portal** to enable end-to-end visibility, governance, and audit readiness of the Organization's DPDP compliance program. The portal shall serve as the **single system of record** for DPDP compliance and shall, at a minimum, support the following capabilities:

a) Progress Tracking & Governance Dashboards

- Phase-wise and activity-wise progress tracking against the approved DPDP roadmap
- Real-time dashboards for Management, DPO, Legal, IT, Risk, and Business stakeholders
- KPI and SLA tracking for consent management, grievance redressal, breach notification, DPIA, and vendor compliance
- Automated alerts for overdue actions, SLA breaches, and regulatory risk indicators

b) Artifact & Evidence Management

- Central repository for all DPDP artefacts including policies, SOPs, DPIAs, ROPA, consent records, vendor assessments, audit reports, and breach logs
- Version control, approval workflows, and change history for all artefacts
- Secure, role-based access to evidence for audit and regulatory inspections
- Tagging and linkage of artefacts to relevant DPDP Act sections and Rules

c) Collaboration & Workflow Management

- Task assignment, dependency tracking, and closure workflows across business, IT, legal, and vendor teams
- In-platform collaboration features including comments, clarifications, and document review
- Escalation workflows aligned to DPDP governance and DPO oversight
- Support for internal and external stakeholders (e.g., consultants, auditors) with controlled access

d) Audit, Inspection & Regulator Readiness

- On-demand generation of audit packs and compliance reports
- Evidence traceability from regulatory obligation → control → artefact
- Time-stamped logs demonstrating accountability and due diligence

e) Security, Scalability & Integration

- Role-based access control and secure authentication
- Scalability to support large user bases including employees, agents, and intermediaries
- Capability to integrate with existing enterprise systems such as IAM, HRMS, Agency Management Systems, ticketing tools, or document management platforms, where applicable

All configurations, dashboards, workflows, and artefacts created under this activity shall be **owned by the LIC**, and the portal shall be capable of continued use beyond the Consultant's engagement.

Only the Hardware (VMs), Network Infrastructure, JBoss Enterprise Application Server, RHEL OS, MySQL (if required), will be provisioned for this by LIC on own premise data center, rest all is to be provisioned by Consultant.

Ownership, administrative access, and all artefacts developed under this activity shall vest with LIC.

1.8 Post Implementation (Operations & Assurance)- Support in managing privacy operations. The activities will include-

- Providing assistance to the DPO office
- Assisting the DPO office in operational activities
- Assistance in planning monthly meetings with the Board and its Committee
- Monitoring the KPIs of the DPO office
- Review and updating of existing in-scope data privacy procedures in alignment with DPDPA
- Assistance in compliance with final DPDP rules, including:
- Designing of FAQs for handling of data principal rights management procedure
- Marketing communication script
- Social media disclaimers
- Online data principal rights form
- DPIA execution and monitoring
- Internal and third-party audits
- Regulatory inspection support as per DPDP Act and other laws of the land.
- Continuous compliance monitoring and dashboards
- Data Breach communication to Data Protection Board of India and affected Data Principal.
- Incident management and response framework
- Establishment of periodic DPDP compliance reporting mechanism to senior management and appropriate board level/committee of LIC
- Perform PBD (Privacy by Design)
- Respond to Data Principle Access Rights
- Provide PMC (Project Management Consultant) support for any privacy tool/technology implementation
- Revalidation/Reassessment to validate closure of gaps identified in the initial Gap Assessment & DPIA exercise.
- DPDP awareness and implementation portal
- Operations, Training and compliance assurance as mentioned in the point 1.7
- Update and Implement amendments as per DPDP Act and Rules.

1.9. Deliverables

- Gap Assessment Report
- Implementation Roadmap
- Applicability Assessment Report
- Personal Data Inventory and Data Flow Diagrams
- Privacy Framework, Policies and SOPs
- Notices and Consent Templates
- DPIA Reports
- ROPA
- Tool RFP and technical evaluation report.
- Training Materials, workshops, seminars, webinars, advisories and monitor progress
- Governance Dashboards
- Reassessment Report