

Reference of the present LIC IT inventory list tentatively:

Sizing Parameter	Requirement/Count	Remarks
Enterprise	Customers: 30 crores Agents: 14 lakhs Employees: 1.2 lakhs	Bidder is requested to estimate the annual DSR volumes based on the estimates shared.
Applications	450	Approximate count
Database	4,000	Structured data sources
Endpoints	80,000	Approximate count
Servers	8,000	Approximate count
Vendors	500	Approximate number
On-Prem Mail Servers		
Annual Consent Volume to be handled without any latency & delay	3 crore/year	10% YoY increase expected
Peak Concurrent Daily Consent Transactions without any latency or adverse user experience	Up to 10 lakhs	Based on policy issuance volume
DPIAs	Process: 550 Application level: 450	Approximate count
ROPA	Process: 500	Approximate count
DSR	3 crore/year	10% YoY increase expected
Number of users	4000	Approximate count
Number of administrators	350	Approximate count
Number of privacy team members	350	Approximate count
Number of business users	350	Approximate count

Data Privacy Notice Management

Sr no.	Requirements	Compliance (Yes/No)	Remarks
1	Ability to generate configurable, dynamic, contextual, comprehensive and short privacy notices based on product, channel, user journey, and regulatory requirements		
2	Provide downloadable capability for users to download consent receipts/artefacts for transparency		
3	Ensure translation and transliteration of notices into all 22 Indian languages as per Schedule 8 of the Constitution		
4	Audit trail for all consent related activities and notice interactions and same cannot be altered		
5	Ensure identification and notification to Data Principals who consent to outdated versions		
6	Version control and historical traceability of all notices and consent artefacts		
7	Ability to identify users with outdated consent and trigger re-consent workflows		
8	The system shall provide maker-checker workflow for creation, modification, and publishing of privacy notices		
9	The solution shall support geo-location-based notice applicability for jurisdiction-specific compliance		
10	Ability to embed notices dynamically within APIs, SDKs, and microservices-based applications		
11	The system shall support offline notice acknowledgement reconciliation (branch/physical forms digitization)		
12	The solution shall provide legal admissibility of consent artefacts in courts/tribunals		
13	Ability to simulate impact of notice changes on existing consent population		

Sr no.	Deliverables	Compliance (Yes/No)	Remarks
1	Design of notice workflow.		
2	Data Privacy Notice/s (including templates) covering all the purposes and legal basis of personal data being processed by LIC aligned with pan India customer base and regulatory communication requirements as per DPDP Act/rules.		
3	All other functionalities mentioned in the section above.		

Consent Management Platform

Sr no.	Requirements	Compliance (Yes/No)	Remarks
1	End-to-end consent lifecycle management including capture, storage, validation, renewal, revocation, and expiry		
2	The consent management platform should be able to integrate and connect to the national consent stack (e.g., NeGD Consent Framework) and any other platform mandated by Government of India or other Statutory Bodies to centralize consent records and ensure consistency across platforms		
3	The platform must have all the functionalities and objectives at a minimal aligned to the Business Requirements Documents issued by NeGD a division under MeitY on April 15, 2025 available on https://msh.meity.gov.in/whatsnew/ Business Requirement Document for Consent Management		
4	The platform shall be capable to handle consent requests during the peak load of 5 lakhs policy issuance in a day. The Bidder will be responsible to plan and consider the sizing of the infrastructure including the hardware, software and other components accordingly. LIC will not be responsible for any issues related to the sizing related matters.		
5	The Proposed Solution shall support explicit, implicit, opt-in, and opt-out consent models		
6	Provide mechanisms for granular consent at the policy holder level, prospects, employees (on-roll and off-roll), pensioners, agents, intermediaries, vendors, contractors, website visitors, mobile application users, digital journey users, etc. ensuring purpose, sub-purpose, and data category specific consent management as per DPDPA 2023 and all clauses as per the finalized rules effective from November 13, 2025 and any further guidelines/notifications/circular that may be issued by regulatory authorities during the course of the engagement		
7	Centralized enterprise-wide consent repository across applications and channels		
8	Consent collection in the platform should support all three modes of Personal Information input i.e. Digital, Physical that is digitized subsequently, through external consent managers and third-party agencies/application collected in physical/digital format		
9	The Bidder must provide documented ability to interoperate with Consent Managers registered with the Data Protection Board beyond the NeGD BRD alignment including but not limited to consent-evidence exchange, onboarding APIs, revocation transmissions.		
10	The proposed solution shall provide event-driven propagation through webhooks and/ or message queue, publication of consent-state changes, revocations and erasure instructions to downstream systems, with delivery guarantees and replay.		
11	Consent revocation impact handling including automated processing restrictions		
12	The Proposed Solution must specify and implement acceptable verification mechanisms for obtaining digitally verifiable Parental/ Guardian consent for minors & Persons with Disability (PwDs) including but not limited to DigiLocker- issued virtual tokens, reliable identity/ age details already held, or equivalent government-backed mechanisms and should be consistent with the DPDP Act & Rules.		
13	The proposed solution shall have the capability to provide consent SDKs for web, Android, iOS, server-side APIs for batch/ legacy channels		
14	Data Principal Rights workflows (access, correction, erasure, portability, grievance)		
15	Consent withdrawal impact handling (processing halt, anonymization, AI unlearning triggers)		

16	Ensure the CMP consent lifecycle is tightly integrated with Record of Processing Activities (ROPA), automatically retrieving processing activity metadata, validating consent, enforcing purpose limitation, propagating updates across systems, and providing dashboards/reports showing consent coverage linked to ROPA activities		
17	The Proposed Solution shall have the capability to maintain an audit trail of consent records, including timestamps, purposes, and associated processing activities as required under DPDP Act 2023 and Rules 2025		
18	The audit trail of consent records cannot be altered and integrity to be ensured for the same		
19	Detailed logs of consent-related activities to be available in a user-friendly interface customized to regulatory requirement for audits		
20	The Proposed Solution shall support consent reconciliation mechanism across channels to resolve inconsistencies		
21	The Proposed Solution shall provide consent dependency mapping across applications and business processes		
22	Capability to flag unauthorized processing attempts where valid consent is absent		
23	The Proposed Solution shall support purpose limitation enforcement with automated blocking controls		
24	Ability to manage third-party consent sharing and downstream accountability tracking		
25	Capability to generate consent dashboards for regulators including consent aging and revocation trends		
26	The Proposed Solution must provide a clean, intuitive, accessible self-service dashboard for Data Principals to view and manage consent and preferences		
27	The Proposed Solution shall provide bulk consent ingestion and migration tools for legacy systems		
28	Support high-volume throughput for consent validation APIs		
29	The proposed solution must have the capability to integrate the Consent Management platform with all identified channels, including websites, mobile apps, applications, servers, other digital platforms, third-party platforms/ applications and physical forms subsequently digitized to manage the consents on real time basis within the LIC infrastructure.		
30	The Proposed Solution shall have the capability to enable explicit consent collection, storage, and retrieval across all identified channels, including websites, mobile apps, other digital platforms, third-party platforms/applications and physical forms subsequently digitized		
31	Proposed Solution shall support Multilingual (Multi-language) support for Consent as defined in the 8th Schedule of the Constitution of India and support for additional language in case they get further added due to amendments		
32	Proposed solution shall enable users to set granular preferences for purposes as per requirements determined by business departments		
33	Support for incorporating consent templates based on business requirements		
34	Implement mechanism for obtaining digitally verifiable consent from Persons with Disability (PwDs) and illiterates		
35	Design, collect and manage consents as per DPDP Act, 2023, Rules 2025 and other relevant regulatory requirements e.g. Insurance Regulatory & Development Authority of India (IRDAI), etc.		
36	Proposed Solution shall have Low-latency operations for real-time consent capture and verification		
37	Support for hierarchical consent structures based on purposes and user attributes, specific data types or purposes etc.		
38	Consent record with timestamp, purpose, and data shared		
39	Consent revocation tracking and enforcement		
40	Automated consent lifecycle management, from collection, storage, expiration, renewal, revocation, logs, security (immutability), and auditability		
41	Centralized repository for managing user consents		
42	Proposed Solution shall support for self-service consent revocation		

43	Proposed Solution shall have feature for secure deletion of consent records upon user request or expiry		
44	Proposed Solution shall have feature for Real-time consent updates and synchronization across systems		
45	Ensure that consent artefacts are immutable, admissible in court, and meet regulatory standards as per MeitY's Electronic Consent Framework		
46	Implement consent retention and expiration mechanisms as per legal and regulatory requirements		
47	The Proposed Solution must support consent nominations and their capture/maintenance in line with DPDP Act and Rules		
48	Maintain consent versions with date and time stamp and ability to track changes in consent forms		
49	The Proposed Solution shall record and store multiple versions of consent agreements and maintain historical consent changes for audits		
50	Consent revalidation after a defined period of time to keep it relevant		
51	Capability to trigger necessary communications (Email/SMS/WhatsApp/in-app/Agentic AI Bots) for expired/expiring consent		
52	Capability to rollout Privacy Notices in all Regional languages mentioned in Schedule 8 of Indian Constitution to legacy/existing customers digitally and record/store their consent		
53	The Proposed Solution should have the capability to ensure clear and transparent communication with users regarding their consent choices and data usage		
54	The Proposed Solution shall have Customizable consent forms like Branding options (logos, themes), Dynamic content based on user location or preferences etc.		
55	The Proposed Solution shall have feature for Real-time reporting on consent metrics like consent rates, revocation trends, Geographic distribution of consents etc.		
56	Consent based access control with technical safeguard for data processing		
57	Enable syncing of updated consent records with internal and external systems		
58	The Proposed Solution must support multi device and multi-channel consent synchronization across web, app, kiosk, chat bot and future digital interfaces to ensure consistency and compliance across all user touch points		
59	Implement robust security measures such as encryption, access controls, and secure data handling practices to protect consent artefacts/user data		
60	The Proposed Solution should be scalable to handle increasing volumes of consent data as the organization grows		
61	Provide an intuitive interface for users to easily manage their consent preferences		
62	The Proposed Solution must support portability of consent data whenever required		
63	The product should include all features necessary to ensure that retrospective consent is captured in accordance with the Act.		
64	Consent identifiers need to be generated by the proposed platform. Bidder to ensure the flexibility in the tool.		
Sr no.	Deliverables	Compliance (Yes/No)	Remarks
1	Design of consent collection, modification and withdrawal workflow.		
2	Consent Management Framework including dashboards for LIC and Data Principals complying with the regulatory requirements as per DPDP Act/rules.		
3	All other functionalities mentioned in the section above.		

Cookie Consent Management

Sr no.	Requirements	Compliance (Yes/No)	Remarks
1	Automated scanning and classification of cookies across web and mobile assets as per regulatory requirements (example - Auto-categorization of cookies into essential, functional, analytics, marketing and performance)		
2	Consent-based blocking/activation of scripts and trackers including 3rd party scripts and tags, based on consent provided by the user		
3	As mandated by the DPDP Act, cookie notices/banners must be drafted by using clear, plain language describing cookie types, purposes, and data collected		
4	Auto-translation of cookie banner content into 22 languages as mandated by the DPDP Act		
5	Deploy a user friendly cookie banner ensuring consent is freely given, specific, informed, and unambiguous		
6	Real-time modification/withdrawal of cookie consent by users		
7	Provide a dedicated section to manage cookie preferences and withdraw consent at any time with equal ease as giving consent		
8	Comprehensive cookie policy to be maintained detailing types, purposes, data collected, retention periods, and third party sharing; review/update regularly for DPDP compliance		
9	Compliance with global consent frameworks where applicable		
10	The solution shall provide continuous monitoring of newly introduced cookies/scripts		
11	Capability to auto-block non-compliant third-party trackers		
12	Ability to generate cookie-level audit trails for forensic purposes		
13	Support for cross-domain and cross-device consent synchronization		
14	Cookie management is required for all applications.		

Sr no.	Deliverables	Compliance (Yes/No)	Remarks
1	Cookie notices/ banners in clear, plain language describing cookie types, purposes, and personal data collected.		
2	Real-time dashboard for modification/withdrawal of cookie consent by users.		
3	All other functionalities mentioned in the section above.		

Data Discovery & Mapping

Sr no.	Requirements	Compliance (Yes/No)	Remarks
1	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		
2	Perform Automated Asset Discovery through agent-based / agent less scans for discovery of the enterprise-wide assets including but not limited to Desktops, Laptops, Servers, etc.		
3	Automatically discover and identify personal data (structured and unstructured) across storage repositories including but not limited to databases, applications, file systems, endpoints, APIs, servers, backup media, tapes and cloud environments		
4	Classify data based on sensitivity, risk, purpose of processing, and retention requirements, aligned with the organization's data classification policy and DPDP obligations		
5	Support identification of high-risk personal data and enable risk-based tagging to facilitate DPIAs and enhanced safeguards		
6	Support linkage of classified data with consent status and purpose limitation and highlight deviations		
7	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		
8	The bidder shall provide all necessary tools, utilities, and resources required for this activity, with no dependency on LIC for tools, licenses, or infrastructure		
9	The bidder shall deliver deployed scanners/collectors	Deleted	Deleted
10	Coverage evidence and completeness reporting including source inventory lists, run IDs, scan completion metrics, success/failure rates, and scan logs suitable for audit review		
11	Agent-based and/or agentless collectors supporting file shares, SharePoint/OneDrive, mail archives, databases, cloud object storage, etc.		
12	Automatic discovery of new databases and tables, and inclusion in scheduled scans		
13	Creation of enterprise Personal Data Inventory and Data Dictionary		
14	AI/ML-powered scanning of structured and unstructured data		
15	Identification of personal data across all systems		
16	Support rule-based and risk-based categorization and tagging		
17	Identification of personal data, children and PwD data. Age verification mechanisms		
18	Mapping of end-to-end data flows (collection → processing → storage → sharing → archival → erasure)		
19	Identification of cross-border data processing		
20	Identification of Single Source of Truth opportunities		
21	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		
22	The Proposed Solution should support scalable and configurable scanning aligned with the LIC's data landscape		
23	Build a unified catalog of data from existing applications on premises and hosted on cloud		
24	Enrich each record with metadata, usage statistics, and ownership details for clear accountability		
25	The Proposed Solution shall support persistent labelling and metadata management such that classification follows the data throughout its lifecycle, including creation, storage, usage, sharing, archival, and disposal		
26	Audit trails must be maintained for classification, reclassification, and labelling changes		
27	Classification tags must be retained during data movement and replication		
28	Application of persistent labels and metadata attributes to identified data assets		
29	Policy-based actions must be enabled and triggered by classification levels		
30	Apply contextual tags (personal, non personal) that map data to business processes and compliance needs		
31	Catalogue (Data fields), Classify (Personal / Non Personal and Categorize (Sensitive Personal, PII)		
32	Provide end to end lineage of data flow across Source, Upstream and Down Stream systems within and outside LIC's interconnected third party ecosystem		
33	Quantifiable risk scoring and index using statistical/transformer-based models		

34	Customizable scanning parameters for data governance and risk management		
35	The Proposed Solution shall be aligned with LIC's security architecture and governance framework		
36	Support API-based integration with encryption, etc., for downstream enforcement of classification policies		
37	Integrate with SIEM/SOC platforms for monitoring classification-related events and anomalies		
38	Integrate with Identity & Access Management (IDAM), Privileged Access Management (PAM) systems for role-based classification governance		
39	Coverage of LIC's entire data footprint, including structured databases, semi structured databases, unstructured databases, cloud data stores, SaaS applications, on-premise data stores, big data platforms, messaging and email platforms		
40	Provide functionality to automate compliance activities and use data responsibly		
41	Provide functionality to protect personal data as per categorization by integrating with Data Protection cyber applications		
42	Intelligently discover, catalogue, classify and categorize data to gain central visibility into data risk		
43	Integrate with cyber protection security posture through automated policy orchestration and remediation actions		
44	Continuously scan and maintain a complete and accurate inventory of data sources across the LIC application ecosystem		

45	The Proposed Solution shall provide centralized dashboards and reporting capabilities to maintain visibility over the LIC data inventory and classification posture		
46	The Proposed Solution shall maintain an up-to-date inventory of identified personal data assets		
47	The Proposed Solution shall provide visibility into high-risk or overexposed data repositories		
48	Support data lineage and flow visualization for impact assessment and regulatory reporting		
49	The Proposed Solution shall generate audit-ready reports aligned with DPDPA and other applicable regulatory frameworks		
50	The Proposed Solution shall generate any other reports required by the regulators/LIC		
51	Support privacy-by-design and data minimization principles		
52	The Proposed Solution shall highlight personal data retained beyond defined retention periods as per LIC policy/regulatory requirements		
53	The Proposed Solution shall support identification of high-risk processing activities requiring further risk assessment or DPIA		
54	The Proposed Solution shall support continuous monitoring and governance of classification controls		
55	Maintain comprehensive logs of scanning activities and classification outcomes		
56	Logs must be accessible for audit, compliance investigations, and forensic review		
57	Detect newly created or modified personal data and automatically apply classification		
58	Enable periodic re-scanning and re-classification of data assets		
59	Provide alerts for unclassified, misclassified, or newly discovered personal data		
60	Operationalize enterprise Data Standards covering data control requirements, data classification, data flows, data quality, and privacy definitions to ensure consistent interpretation and compliance across the organization		
61	Establish a systematic approach for data classification and mapping across LIC, providing clarity on data types, their usage, and controls applied across the data lifecycle		
62	Ensure security, data accuracy, integrity, and security throughout the data lifecycle via defined standards, controls, and ongoing monitoring mechanisms		
63	The Proposed Solution must allow users to classify emails in mailbox folders manually or automatically		
64	Email classification must enforce recipient validation (e.g., prevent "Internal" classified emails from being sent externally)		
65	The Proposed Solution must integrate with Active Directory, etc. to enforce role based and department based classification policies		
66	OCR capability must be available for discovery within scanned documents and images		
67	The Proposed Solution must support discovery of sensitive data in image based documents		
68	The ability of the Proposed Solution to detect sensitive data in nested files and compressed archives is desirable		
69	The Proposed Solution must support template matching and similarity based document detection for classification		
70	The Proposed Solution must support AI/ML-assisted discovery and classification. The AI engine must be deployable within LIC infrastructure and be trainable using LIC-specific datasets		
71	The Proposed Solution must provide a web based centralized administration portal supporting unlimited policy creation and configuration		
72	The Proposed Solution must support tagging/marking specific sensitive data elements to enable regulatory and internal reporting requirements		
73	The Proposed Solution shall provide a centralized inventory view of discovered data by type, location, owner, classification level, etc.		
74	The Proposed Solution must provide risk scoring and prioritization based on data sensitivity, exposure levels, repository risk indicators, etc.		
75	The Proposed Solution must provide searchable discovery results with advanced filtering and query capabilities across repositories		
76	The Proposed Solution will support LIC in adopting secure methods for storing, retrieving, and disposing of sensitive data		
77	Identify high risk processes, departments, and assets involved in high risk personal data processing to prioritize security measures		

78	Conduct stakeholder walkthroughs to map personal data flow within key business processes, identifying associated applications and infrastructure		
79	Analyse and mitigate risks associated with data security during transit, use, and storage; identify and address risks tied to departmental/branch storage practices		
80	The Proposed Solution shall enable ingestion, synchronization, and exchange of metadata with all applications using standard interfaces, APIs, or connectors		
81	The Proposed Solution must preserve and align with existing data governance structures, including data lineage, classifications, stewardship roles, etc. maintained within LIC		
82	Integration must not disrupt current LIC operations. The solution should support real-time or scheduled metadata updates and ensure continuity of data catalog services		
83	The bidder shall provide detailed documentation outlining the technical approach for integration, including any dependencies, customization requirements, and limitations		
84	The integration must adhere to industry best practices and standards for metadata management, data governance, and interoperability. The data discovery tool must have the capability to incorporate new applications as and when they are introduced during the engagement period		

Sr no.	Deliverables	Compliance (Yes/No)	Remarks
1	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.		
2	Automatically discover and identify personal data (structured, semi structured and unstructured) across storage repositories including but not limited to databases, applications, file systems, endpoints, APIs, servers, backup media, tapes and cloud environments		
3	All other functionalities mentioned in the section above.		

Data Principal Rights Management

Sr no.	Requirements	Compliance (Yes/No)	Remarks
1	Self-service user friendly portal for Data Principals to view and manage their rights		
2	Multi-channel request intake (web, mobile, branch, call center)		
3	Workflow orchestration for rights requests as per DPDPA, including Right to Access Consent/Personal Data, Right to Revoke Consent, Right to Correction and Erasure of Data including third-party workflow integrations, Right to Grievance Redressal, and Right to Nominate (in the event of death or incapacity)		
4	The Proposed Solution shall deliver an end-to-end automated Data Principal Rights Management (DPRM) System that will be fully aligned with the DPDP Act, applicable Rules, and LIC internal policies		
5	The Proposed Solution shall maintain immutable audit trails documenting every stage of request handling		
6	The Proposed Solution shall provide ready to use and standardized response templates for all the Data Principal Rights as per DPDP Act and further ensuring compliance with statutory content requirements		
7	Provide a structured framework for nominee management covering capture, validation, update, and revocation processes, that can enable nominees to exercise their rights in accordance with DPDP Act, Rules and LIC Terms of Service		
8	The Proposed Solution shall provide comprehensive documentation reporting capabilities to management and regulators, including exporting documentation in formats like CSV, PDF, etc. for Board-level oversight and regulatory inquiries		
9	Configure operational SLAs to align with the statutory 90-day grievance resolution requirement as per DPDP Act and LIC defined service thresholds along with timely notifications		
10	The bidder shall deliver supporting policies, Standard Operating Procedures, RACI matrices, and structured training programs		
11	Identity verification and authentication mechanisms		
12	The Proposed Solution shall have the capability to enforce identity verification protocols for Data Principals submitting requests to prevent unauthorized access or fraudulent requests		
13	Maintain a centralized register/tracker to record all Data Principal Requests, responses, and resolution times, demonstrating compliance		
14	The Proposed Solution shall implement a system to receive, track, manage, and respond to Data Principal rights requests efficiently and accurately		
15	Integration and operationalization of Data Principal rights and grievance handling post assessment of LIC existing setup		
16	The Proposed Solution shall support the capture of Data Principal rights requests initiated at any branch of LIC, service point, or other assisted channel defined by LIC, ensuring full compliance with DPDP Act/Rules		
17	The Proposed Solution developed for capturing rights requests at branches, etc. on behalf of the customer, shall have verifiable audit trails with maker/checker facility. Such requests may be digitized into the system as per process flow designed in consultation with LIC		
18	Capability to handle bulk requests during surge scenarios (e.g., campaigns, regulatory triggers)		
19	The Proposed Solution shall support exception handling workflows (request rejection, partial fulfilment)		
20	Ability to process requests spanning multiple legal entities/subsidiaries		
21	Automated orchestration across multiple applications and vendors		
22	Real-time status tracking with audit trails		
23	Multi-channel notifications to Data Principals (SMS, email, app, etc.)		
24	The Proposed Solution shall provide automated deduplication of multiple requests from the same individual		
25	Capability to track and report reason codes for denial of requests		
26	Ability to generate regulatory submission reports for grievance handling		
27	Integration with outsourced vendors for fulfillment tracking		
28	Data Principals should be able to download a copy of their consent history		
29	Ensure clear and transparent communication with Data Principals throughout the request process		

30	The Proposed Solution shall use automated tools/mechanisms to securely collate requested information and reduce manual effort and errors while fulfilling Data Principal requests		
31	The Proposed Solution shall assist relevant teams in identifying databases/systems that must be queried or accessed to respond to access requests		
32	The Proposed Solution shall be able to create and maintain a centralized, secure repository documenting processing activities, including purposes of processing, categories of Data Principals and categories of personal data, data recipients, data transfers, and retention periods		
33	The Proposal Solution shall analyze and integrate existing grievance redressal systems to ensure all data privacy related grievances can be centrally received, acknowledged, tracked, and responded to within required timelines as per LIC policy		
34	The Proposed Solution shall have the capability to create or enhance a grievance redressal workflow/process to meet the grievance timelines issued by the DPDP Rules (90 days) or LIC specified timelines (whichever is earlier and applicable)		
35	The Proposed Solution shall establish a mechanism to enable Data Principals to nominate one or more individuals who may exercise the Data Principal rights in the event of death/incapacity, aligned to DPDP Act 2023, applicable Rules, LIC terms of service and applicable laws		
36	The Proposed Solution shall have the capability to implement system functionality to securely capture and manage nomination details, including required particulars and identity validation of nominated individuals through means specified by LIC		
37	The Proposed Solution shall ensure the system enables verified nominees to exercise Data Principal rights upon death/incapacity in accordance with DPDP Act 2023, applicable Rules, and LIC terms and services		
38	Implement workflows which should be configurable to streamline the entire process at LIC to receive, verify, respond to, and process these requests efficiently		
39	Ensure view consent and revoke consent requests could be handled in a self-service manner to reduce number of tickets handled by privacy team or DPO office		
40	Seamless integration with existing systems and data sources to facilitate efficient data discovery and retrieval		
41	The proposed solution shall have the capability to provide an algorithmic due-diligence register documenting checks that the algorithmic/ AI processing will not risk the Data Principal Rights		

Sr no.	Deliverables	Compliance (Yes/No)	Remarks
1	Data Principal Rights Management Framework as per DPDP regulations including but not limited to templates, procedures, automated response mechanism/ templates on Data Principal Rights, identity verification of Data Principals.		
2	All other functionalities mentioned in the section above		

Data Protection Impact Assessment

Sr no.	Requirements	Compliance (Yes/No)	Remarks
1	Configurable DPIA templates aligned with DPDP Act		
2	Configurable risk rules and thresholds within the ROPA so that any addition or change to a processing activity that meets high risk criteria will automatically initiate or refresh a DPIA		
3	DPIA initiation/refresh must support pre population of DPIA inputs from the associated ROPA record		
4	The proposed solution must be able to perform automated annual DPIAs to comply with the Significant Data Fiduciary requirement of performing an annual DPIAs and its submission to the DPB.		
5	Multi-level approval workflows with role-based access control		
6	DPIA initiation/refresh must support role-based approvals with documented decision history		
7	Automated risk scoring and categorization		
8	Automated workflows for conducting DPIAs		
9	Integration with data discovery and mapping modules, business processes		
10	Ability to trigger DPIA for new products, changes, or processing activities		
11	The Proposed Solution must maintain complete, immutable audit trails for all ROPA changes, DPIA triggers, DPIA workflow actions, approvals/rejections, and finalization events		
12	AI-assisted or rule-based auto-population of DPIA forms		
13	The Proposed Solution shall support threshold-based automatic triggering of DPIA		
14	The Proposed Solution shall be capable of generating comprehensive reports detailing the assessment process, including nature, scope, context, and purposes of processing		
15	The Proposed Solution shall be capable of generating DPIA reports that include identified risks, risk scoring/evaluation outcomes, mitigation recommendations, workflow approvals, and audit evidence		
16	Capability to maintain DPIA library for reuse across similar processes		
17	Provide notifications to relevant stakeholders for DPIA initiation, pending approvals, overdue actions, and completion		
18	Provide management dashboards and exports showing DPIA status, including pending/overdue DPIAs, completion status, and trend/summary reporting for oversight		
19	Ability to map risk mitigation actions to control libraries		
20	The solution shall support residual risk calculation post-control implementation governance		
21	Evidence management and document repository		
22	Automated reminders, escalations, and tracking		
23	Ability to share DPIA outputs with vendors and regulators		
24	The Proposed Solution shall provide audit trail for all DPIA modifications and approvals		
25	The Proposed Solution must have the capability of workflow automation for DPIA approvals, stakeholder collaboration, version control, and audit trails, minimizing manual overhead and ensuring governance fidelity		

26	Risk Categorization Matrix must be prepared through the tool with measurement criteria based on risk analysis during DPIA and Data Privacy risk assessment and develop a treatment plan for data privacy-related risks identified. Implement measures to address identified risks and ensure compliance with the LIC Policy, DPDP Act/Rules		
27	Capability to generate regulatory-ready DPIA reports		
28	The Proposed Solution shall assist in obtaining approvals and signoffs from the Data Protection Officer before releasing the reports		
29	Ability to track overdue DPIAs and escalate to management		
30	Dashboard should provide real time visibility into the initiation, review, approval and closure of DPIAs across all Branches and Business functions		
31	The Proposed Solution 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		
32	Support for automated alerts and escalations to DPOs, Privacy Stewards, or relevant functionaries in case of SLA breaches or pending approvals		
33	Ability to generate compliance scorecards and dashboards for each branch, Region, Zone, Department or business Vertical		
34	The platform must be scalable to onboard all branches and new privacy stakeholders as per future organizational requirements		

Sr no.	Deliverables	Compliance (Yes/No)	Remarks
1	Data Principal Rights Management Framework as per DPDP regulations including but not limited to templates, procedures, automated response mechanism/ templates on Data Principal Rights, identity verification of Data Principals.		
2	All other functionalities mentioned in the section above.		

Record of Processing Activities (ROPA) - automated & integrated to DPIA

Sr no.	Requirements	Compliance (Yes/No)	Remarks
1	Automated creation of ROPA based on data discovery and DPIA outputs		
2	Configure and deliver a comprehensive Records of Processing Activities (ROPA) solution including but not limited to covering all applications, systems, business processes, and third-party vendors across the enterprise		
3	The Proposed Solution shall maintain a centralized and structured inventory of all personal data processing activities and incorporate processing risk assessment (DPIA) as an integral component of the ROPA framework to ensure visibility of associated privacy and data protection risks in alignment with the DPDP Act and Rules		
4	Structured workflows to be implemented to capture, validate, review, and approve processing records		
5	Centralized repository for all processing activities		
6	Real-time updates based on system/data changes		
7	The Proposed Solution must capture key attributes including processing purposes, data categories and elements, recipients/processors, cross-border transfers, retention schedules, and implemented safeguards in alignment with LIC Policy, DPDP Act and DPDP Rules requirements		
8	Linkage with consent, DPIA, and data mapping modules		
9	The Proposed Solution must ensure that the ROPA records are kept accurate, up to date, and complete, with validation mechanisms and regular updates to keep records current		
10	The Proposed Solution must have the capability to dynamically maintain via automated feeds and workflows enabling continuous refresh of processing records based on defined sources of change (e.g., system onboarding, process changes, vendor additions, retention updates, etc.)		
11	The Proposed Solution must be able to provide configurable options to wire automated feeds from change sources into the ROPA and maintain traceable updates to processing activities		
12	Versioning and historical tracking of processing records		
13	The Proposed Solution shall have end-to-end ROPA entry capability that enables creation of a new processing activity capturing purpose, categories, data elements, processors, transfers, retention, safeguards, etc.		
14	The Proposed Solution shall have end-to-end ROPA entry capability that enforces required approval prior to finalizing/activating an entry		

15	The Proposed Solution shall have end-to-end ROPA entry capability that records the full lifecycle (create/update/approve/reject/export etc.) in immutable audit logs with user, timestamp, action, and before/after change metadata		
16	The Proposed Solution shall support automated reconciliation between ROPA and actual system processing		
17	Capability to highlight inconsistencies between declared and actual processing activities		
18	Ability to link ROPA entries to vendor contracts and third-party agreements		
19	The Proposed Solution shall have the capability to configure automated risk triggers for qualifying changes (e.g., new purposes, personal data categories, transfers etc.), initiating or refreshing DPIAs with RBAC-based approvals, evidence capture, and dashboard visibility, aligned to SDF obligations		
20	The Proposed Solution shall support end-to-end integration with CMP workflows, automatically retrieving consent metadata for each processing activity, validating lawful basis and purpose alignment, triggering DPIAs for high-risk changes, maintaining immutable audit trails, and providing dashboards/reports showing consent coverage, processing activity alignment, and risk assessment outcomes		
21	The Proposed Solution shall have the capability to assign clear ownership and responsibility for maintaining and updating ROPA entries to ensure accuracy and completeness (e.g., defined roles such as ROPA admins/stewards, process owners, reviewers/approvers)		
22	Tamper-proof audit-ready records with full traceability		
23	The Proposed Solution must capture and maintain a structured database of processing activities including, but not limited to: nature, scope, context, and purposes of processing; purposes of processing and legal basis; categories of Data Principals; categories of data processors (as applicable); types/categories of personal data processed; data transfers (wherever applicable); data recipients (wherever relevant); security measures/security practices; and retention periods/retention schedules		
24	The Proposed Solution must support detailed logs and reporting on data handling practices, including security measures and controls applied to processing activities		
25	The Proposed Solution shall ensure defensibility of ROPA in regulatory inspections		
26	Capability to generate custom ROPA extracts for regulator-specific formats		
27	The bidder shall provide supporting templates, UAT scripts, structured training sessions, policies, SOPs, templates and post-go-live hyper care support to ensure sustainable adoption and compliance		

Sr no.	Deliverables	Compliance (Yes/No)	Remarks
1	Automated creation of ROPA, including but not limited to covering all applications, systems, business processes, and third-party vendors across the enterprise.		
2	Automation of RoPA should be based on data discovery and DPIA outputs and its integration with DPIA.		
3	All other functionalities mentioned in the section above in compliance with the DPDP regulation.		

Personal Data Breach Management

Sr no.	Requirements	Compliance (Yes/No)	Remarks
1	The bidder shall implement a solution for personal data breach detection, management and reporting, in line with the requirements of the Digital Personal Data Protection (DPDP) Act, 2023, and the Rules 2025		
2	The Proposed Solution should have the capability to notify Data Protection Board of India (DPBI) and the Data Principals within the prescribed timeframe as per the DPDP Act, 2023 and Rules 2025		
3	The Proposed Solution shall maintain centralized records of all reported breaches for compliance verification and audit		
4	Configurable notification templates for stakeholders and customers		
5	Cohort-based identification of impacted data subjects		
6	The Proposed Solution shall have the capability to share initial and final breach reports to both impacted Data Principals and DPBI		
7	The Proposed Solution shall assist in implementing a robust breach management framework that enables timely detection, assessment, reporting, and mitigation of personal data breaches		
8	The Proposed Solution shall have the capability in implementing real-time breach detection by integrating with the EDR, SIEM, SOAR, DLP, IDS/IPS, IDAM, PAMS, LIC incident management and anomaly detection tools for automated event ingestion		
9	The Proposed Solution shall define breach indicators for unauthorized access, exfiltration, modification or misuse of personal data		
10	The Proposed Solution shall maintain tamper-proof logs of all security events affecting personal data		
11	The Proposed Solution shall have the capability to conduct forensic analysis to determine the origin, scope, and impact of the breach		
12	Maintain a structured evidence collection process to support legal and regulatory investigations		
13	Capability to generate impact heatmaps for affected users/data types		
14	Ability to simulate worst-case exposure scenarios		
15	The Proposed Solution must be able to integrate a breach management solution with existing SOC and SIEM platform for alerting, managing, investigating, and reporting personal data breaches to Data Fiduciary, Data Principal and DPBI		

16	The Proposed Solution shall have the capability to classify breaches based on severity (Personal Data Breach/Sensitive Personal Data Breach, etc.), type of data compromised, number of Data Principals affected, and potential impact		
17	The Proposed Solution shall have the capability to support automatic bulk generation and dispatch of notices across channels (email/SMS/WhatsApp/in-app etc.) using templated content that includes required breach details and customer remediation steps		
18	The Proposed Solution shall provide connectors/workflows to submit DPDP notifications via regulator endpoints/portal		
19	The Proposed Solution shall have the installation capability across on-premises, cloud, hybrid environments, and third-party service providers		
20	The Proposed Solution must cover all the applicable and in-scope personal data collected and processed by LIC, including the personal data exchanged with third-party entities		
21	The Proposed Solution must have the required alerting capabilities for personal data breaches/breach attempts across all the processes and technologies in LIC that collect and process personal information		
22	The Proposed Solution shall expose bounce/failure handling, renotification as needed, delivery status, and dashboards displaying who was notified		
23	The Proposed Solution shall have the capability to operationalize the DPB intimation under the Rules as follows: i. An immediate/ without-delay initial intimation ii. A detailed report within the 72 hour window – with workflow timers, evidence capture and template with content which should cover including but not limited to the nature, extent, timing, likely consequences, mitigation, , number of data principals affected, remediation, etc.		
24	The Proposed Solution shall ensure rapid recovery of affected systems and data using secure backup and restoration mechanisms		
25	The Proposed Solution shall have the capability to conduct a post-breach review to identify gaps in security controls		
26	The Proposed Solution must be in compliance with regulatory requirements including but not limited to DPDP Act and Rules, IRDAI, CERT-In, ISO 27001, and NIST Frameworks		
27	The Proposed Solution should be able to automatically notify the affected Data Principals promptly, including nature of the breach, mitigation steps taken, recommended actions to prevent harm, and types of personal data compromised		
28	Capability to track repeat incidents and systemic weaknesses		
29	Integration capabilities with enterprise risk management systems		

Sr no.	Deliverables	Compliance (Yes/No)	Remarks
1	Implement the Personal Data Breach Management solution for personal data breach detection, management and reporting, in line with the requirements of the Digital Personal Data Protection (DPDP) Act, 2023, and the Rules 2025.		
2	Configurable notification templates for stakeholders including DPBI and customers.		
3	All other functionalities mentioned in the section above in compliance with the DPDP regulation.		

Third Party Vendor Risk Management

Sr no.	Requirements	Compliance (Yes/No)	Remarks
1	The Proposed Solution must be in compliance with regulatory requirements including but not limited to DPDP Act and Rules, IRDAI, ISO 27001, and NIST Frameworks.		
2	The Proposed Solution must be able to conduct pre-onboarding and post-onboarding privacy risk assessment of vendors and generate reports.		
3	The Proposed Solution shall have the capability to send reminders automatically on a periodic basis to conduct a refresh audit of existing vendors.		
4	The Proposed Solution shall be able to integrate with existing vendor management and contract management systems of LIC.		
5	The Proposed Solution shall have the capability to create, assign third-party risk assessments to vendors and manage the lifecycle.		
6	The Proposed Solution shall have the capability to measure compliance with Data Sharing Agreements and raise alerts to DPO.		
7	The Proposed Solution shall have the capability to create an audit trail with data processors to ensure compliance as per consent updation/revocation by Data Principal.		
8	The Proposed Solution shall have the capability to raise deletion requests to processors.		
9	The Proposed Solution shall be able to route deletion requests from Data Principal Rights Management to processors (both manually and automatically).		
10	The Proposed Solution shall have the capability for Data Processors to acknowledge, upload proofs and comply with deletion requests.		
11	The Proposed Solution shall maintain a list of all the third parties with whom the personal data is shared for processing (both manually and automatically).		
12	The Proposed Solution shall create and maintain an audit checklist.		
13	The Proposed Solution shall have the capability to assign risk scores to vendors based on the audits performed.		
14	The Proposed Solution shall assist with vendor contract remediation and provide standardized DPDP-compliant contractual clauses/templates (Data Processing Agreement).		

Sr no.	Deliverables	Compliance (Yes/No)	Remarks
1	Implement the Third Party Vendor Risk Management Framework including but not limited to vendor audit checklist, vendor audit reports, policies, contractual agreements, compliance requirements in line with the requirements of the Digital Personal Data Protection (DPDP) Act, 2023, and the Rules 2025.		
2	Dashboard of vendors processing personal data shared by LIC along with the status of their compliance.		
3	All other functionalities mentioned in the section above.		

Compliance Reporting & Dashbaords

Sr no.	Requirements	Compliance (Yes/No)	Remarks
1	Real Time Monitoring: Dashboard should provide real time Visibility into the initiation, review, approval and closure of DPIAs across all Branches and Business functions.		
2	SLA Based Time Tracking: The Proposed Solution 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.		
3	Alerts and Escalations: Support for automated alerts and escalations to DPOs, Privacy Stewards, or relevant functionaries in case of SLA breaches or pending approvals.		
4	Branch Wise & Function Wise Compliance Overview: Ability to generate compliance scorecards and dashboards for each branch, Region, Zone, Department or business Vertical.		
5	5)Role-Based Access Controls (RBAC): The Proposed Solution should allow differentiated access for: i. DPO – Global access with configuration and oversight privileges. ii. Privacy Stewards – Access to DPIAs within their assigned branches/ Verticals. iii. Branch/ Region/ Zone – Access to DPIAs initiated or owned by their teams.		
6	6)Role-Based Access Controls (RBAC): The Proposed Solution should allow differentiated access for: i. Privacy Champions/ Stewards – Access to the modules within their assigned branches/ Verticals. ii. Branch/ Region/ Zone – Access to the modules owned by their teams.		
7	The Proposed Solution must be scalable to onboard all branches and new privacy stakeholders as per future organizational requirements.		
8	The Proposed Solution must be able to provide a comprehensive dashboard and further assist the DPO in exporting the summary of the key KPI's required for reporting to the management.		
9	The solution should provide predefined report as well as configurable report as per LIC requirements.		

Sr no.	Deliverables	Compliance (Yes/No)	Remarks
1	Real time monitoring dashboards.		
2	Automated SLA based time tracking and reporting.		
3	Automated Alerts and Escalations.		
4	All other functionalities mentioned in the section above.		

Workflow Management

Sr no.	Requirements	Compliance (Yes/No)	Remarks
1	Task assignment, dependency tracking, and closure workflows across business, IT, legal, and vendor teams.		
2	In-platform collaboration features including comments, clarifications, and document review.		
3	Escalation workflows aligned to DPDP governance and DPO oversight.		
4	Support for internal and external stakeholders (e.g., consultants, auditors) with controlled access.		
5	The proposed solution shall provide configurable end-to-end workflow management to automate DPDP-related processes, including creation, review, approval, modification, and deletion of purposes, consent records, purpose library entries, notices, DPIAs, RoPA, and other privacy artifacts. The solution shall support configurable approval workflows with role-based access control, automatic routing to designated business owners, notifications, reminders, escalations, SLA tracking, status monitoring, and complete audit trails for all workflow activities.		
6	The proposed solution shall provide standard integration capabilities to automatically synchronize newly identified processing purposes, consent requirements, and related metadata with the purpose library. Workflow access shall be provided to all designated business owners and stakeholders.		
7	The proposed solution must be able to provide annual independent audit workflows with evidence packs to comply with the Significant Data Fiduciary requirement of performing annual audits and submission of the audit report to the DPB.		
8	Implement automated workflows to provide: i. secure data disposal when retention periods expire, including secure deletion and evidence logging ii. Purpose wise retention-schedule enforcement, iii. erasure on exhaustion/ withdrawal of purpose and iv. A configurable pre-erasure notice to the Data Principal v. Legal preservation hold capabilities to support privacy and regulatory compliance around retention and disposal of personal data vi. Capability to classify personal data by category and apply retention rules automatically based on data category, purpose, and lifecycle stage. vii. Capability to automatically trigger secure deletion, compliant archiving, and/ or de - identification/anonymization, based on retention schedules and policy rules viii. The capability to ensure retention/deletion actions are auditable and protected against unauthorized changes ix. The capability to integrate data retention and right to erasure workflows with governed lifecycle controls.		
9	The proposed solution shall enforce data retention and deletion policies in line with LIC guidelines, regulatory guidelines and legal requirements.		
10	Three level of approval hierarchies to be configured at departmental level.		

Sr no.	Deliverables	Compliance (Yes/No)	Remarks
1	Task assignment, dependency tracking, Implementation of workflows and closure workflows as mentioned in the requirements section above.		
2	Escalation workflows.		
3	All other functionalities as mentioned in the requirements section above.		

DPDP Program Management Portal

The Bidder 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:

Sr no.	Requirements	Compliance (Yes/No)	Remarks
1	Progress Tracking & Governance Dashboards: 1) Phase-wise and activity-wise progress tracking against the approved DPDP roadmap 2) Real-time dashboards for Management, DPO, Legal, IT, Risk, and Business stakeholders 3) KPI and SLA tracking for consent management, grievance redressal, breach notification, DPIA, and vendor compliance 4) Automated alerts for overdue actions, SLA breaches, and regulatory risk indicators		
2	Artifact & Evidence Management: 1) Central repository for all DPDP artefacts including policies, SOPs, DPIAs, ROPA, consent records, 2) vendor assessments, audit reports, and breach logs 3) Version control, approval workflows, and change history for all artefacts 4) Secure, role-based access to evidence for audit and regulatory inspections 5) Tagging and linkage of artefacts to relevant DPDP Act sections and Rules		
3	Collaboration & Workflow Management: 1) Task assignment, dependency tracking, and closure workflows across business, IT, legal, and vendor teams 2) In-platform collaboration features including comments, clarifications, and document review 3) Escalation workflows aligned to DPDP governance and DPO oversight 4) Support for internal and external stakeholders (e.g., consultants, auditors) with controlled access		
4	Audit, Inspection & Regulator Readiness: 1) On-demand generation of audit packs and compliance reports 2) Evidence traceability from regulatory obligation → control → artefact 3) Time-stamped logs demonstrating accountability and due diligence		
5	Security, Scalability & Integration: 1) Role-based access control and secure authentication 2) Scalability to support large user bases including employees, agents, and intermediaries 3) Capability to integrate with existing enterprise systems such as IAM, HRMS, Agency Management 4) Systems, ticketing tools, or document management platforms, where applicable		

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

Only the RHEL OS, (if required), will be provisioned for this by LIC on own premise data center, rest all is to be provisioned by Bidder.

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

Sr no.	Deliverables	Compliance (Yes/No)	Remarks
1	Progress tracking & Governance Dashboards.		
2	All other functionalities as mentioned in the requirements section above.		