Implementation of

Data Privacy & Consent Management System (DPCMS) in compliance with the Digital Personal Data Protection Act, 2023.

Issued by: Kerala State Cooperative Bank (KSCB)

In collaboration with: Kerala Startup Mission (KSUM)

Reference No-{KBIT/PMU Data
privacy & Consent management
System(DPCMS/088/25-26}

Table of contents

1. Introduction

The Kerala State Cooperative Bank (KSCB), the apex cooperative bank of Kerala, invites proposals from eligible startups registered under Kerala Startup Mission (KSUM) for the design, implementation, hosting, and support of a **comprehensive Data Privacy & Consent Management System (DPCMS**) in compliance with the Digital Personal Data Protection Act, 2023. The proposed initiative aims to establish a robust, technology-enabled privacy governance framework to ensure lawful processing of personal data, strengthen customer trust, and achieve sustained regulatory compliance across the Bank's digital and operational ecosystem. The scope of the DPCMS covers the following solution areas:

Data Discovery & Classification: Implement automated mechanisms to identify, catalogue, and classify personal data across core banking systems, digital channels, enterprise applications, databases, and document repositories. This will enable visibility into data flows, support data minimisation, and facilitate compliance with statutory obligations.

Consent Management: Establish a centralized consent management framework to capture, store, manage, and audit explicit, purpose-specific customer consents across all service channels. The system shall support consent lifecycle management, withdrawal of consent, and integration with customer-facing digital platforms.

Data Principal Rights Management: Deploy structured workflows to enable data principals to exercise their rights under the DPDP Act, including access, correction, erasure, and grievance redressal. The platform shall ensure SLA-driven processing, acknowledgements, escalation, and closure tracking.

Privacy Governance & Compliance Management: Implement governance tools to maintain Records of Processing Activities (RoPA), enforce purpose limitation and data retention policies, and map internal controls to DPDP Act provisions. The system shall generate audit-ready evidence for regulatory inspections and internal reviews.

Data Breach & Incident Management: Establish an integrated incident management module to detect, log, assess, and respond to personal data breaches. The solution shall support regulatory reporting timelines, root-cause analysis, corrective action tracking, and management reporting.

Reporting & Dashboards: Provide role-based dashboards and reports for the Board, senior management, IT, and compliance teams to monitor privacy posture, compliance status, risk indicators, and remediation actions in a timely and transparent manner.

The DPCMS shall be implemented in a CAPEX model and shall be scalable, API-first, multilingual, and interoperable with existing and future banking systems. The solution must comply with DPDP Act, NABARD cyber security framework, RBI advisories, and Meity/CERT-In directions, and support seamless integration with national and Kerala state digital platforms to ensure long-term regulatory alignment and operational resilience.

2. Objectives

- ✧ Implement a centralized Data Privacy & Consent Management System (DPCMS) to ensure full compliance with the Digital Personal Data Protection Act, 2023 across all banking operations and digital channels.
- ✧ Establish compliance-by-design privacy controls aligned with DPDP Act, RBI cyber security framework, NABARD advisories, and CERT-In directions.
- ✧ Enable automated data discovery, classification, and mapping of personal data across CBS, digital banking platforms, enterprise applications, and third-party integrations.
- ✧ Deploy an enterprise-wide consent management framework supporting purpose limitation, consent lifecycle management, and auditability.
- ✧ Enable structured, SLA-driven Data Principal rights management including access, correction, erasure, consent withdrawal, and grievance redressal.
- ✧ Implement privacy governance and accountability mechanisms, including Records of Processing Activities (RoPA), data retention controls, and audit-ready evidence generation.
- ✧ Establish an integrated data breach and incident management framework to support timely detection, assessment, reporting, and remediation as mandated under the DPDP Act.
- ✧ Provide role-based dashboards and regulatory reports for the Board, senior management, IT,

and compliance teams.

- ✧ Integrate seamlessly with Finacle 10.2.25 CBS , allied solutions &digital platforms through secure, API-first architecture.

3. Scope of Work

3.1 Functional Scope

Brief functional scope

Sr No	Features
1.	Universal Consent Management
2.	Cookie Consent
3.	Data Mapping Automation
4.	**Integration with** existing and future banking systems and regulatory systems .
5.	Data Principal Rights Management
6.	Privacy Assessments
7.	Data Protection Impact Assessments
8.	Privacy Notice Management
9.	Data Breach Management
10.	Controls, Reporting and Dashboard
11.	Research Repository on Data Protection Laws

Additional details on functional scope

- ✧ Enterprise-wide data discovery and classification of personal data across Core Banking System (Finacle), Internet Banking, Mobile Banking, UPI, Digital Lending platforms, DMS, HRMS, CRM, and third-party applications.
- ✧ Automated mapping of data processing activities to purpose, legal basis, data category, retention period, and system of record.
- ✧ Centralized consent management covering capture, storage, validation, modification, withdrawal, and audit of explicit and purpose-specific consents.
- ✧ Consent lifecycle management integrated with customer-facing digital channels, branch

operations, and backend systems.

- ✧ Structured Data Principal rights management workflows for access, correction, erasure, consent withdrawal, and grievance redressal as mandated under the DPDP Act 2023 and further amendments .
- ✧ SLA-driven grievance management, acknowledgements, escalation, and closure tracking.

- ✧ Privacy governance and accountability mechanisms including Records of Processing Activities (RoPA), policy mapping, and compliance monitoring.
- ✧ Data retention and deletion management aligned to regulatory, legal, and business requirements
  Integrated personal data breach detection, logging, classification, and response management.
- ✧ Support for regulatory and management reporting, including DPDP compliance status, risk indicators, and remediation tracking
- ✧ Role-based dashboards for Board, senior management, IT, compliance, and audit teams
  Audit trails, logs, and evidence generation to support regulatory inspections and internal audits.
- ✧ Alerts, reminders, and notifications for SLA breaches, consent expiry, pending requests, and compliance actions.
- ✧ Secure document tagging and linkage for privacy notices, consent artefacts, and compliance records.

3.2 Technical Scope in brief

- ✧ API-first, modular, microservices-based architecture supporting seamless integration with existing and future banking systems.
- ✧ Secure integration with CBS, digital banking platforms, DMS, and allied banking solutions.
- ✧ Deployment in CAPEX model .
- ✧ Support for role-based access control (RBAC), multi-factor authentication, and least-privilege principles.
- ✧ Secure data storage, encryption at rest and in transit, and tamper-proof audit logging.
- ✧ Configurable workflow engine for consent management, rights requests, and incident handling.
- ✧ Rules-based orchestration layer to enforce purpose limitation, retention, and compliance-by-design controls.
- ✧ Support for offline data capture and deferred sync where applicable (branch / field operations)
- ✧ High availability, scalability, and disaster recovery support .

- ✧ Compliance with DPDP Act, NABARD cyber security framework, RBI advisories, and CERT-In directions.

3.3 Integration Scope in brief

- ✧ Core Banking System (CBS): Integration for identification of personal data elements, customer profiles, account information, transaction references, consent enforcement, and purpose validation across banking operations.
- ✧ Digital Banking Channels: Integration with Internet Banking, Mobile Banking, UPI, and Digital Lending platforms for real-time consent capture, validation, withdrawal, and audit logging.
- ✧ NPCI Systems: Integration with NPCI platforms (UPI, AEPS, BBPS, RuPay, etc.) to enforce consent-based data sharing, monitor data flows, and support DPDP-aligned audit requirements.
- ✧ Aadhaar Ecosystem: Integration with UIDAI-approved Aadhaar services (e-KYC, offline Aadhaar, XML, VID, QR-based verification) strictly on consent basis and in compliance with UIDAI and DPDP Act guidelines.
- ✧ DigiLocker: Integration with DigiLocker for secure, consent-driven retrieval and verification of customer documents, enabling document minimisation and auditability.
- ✧ Account Aggregator (AA) Framework: Integration with RBI-regulated Account Aggregator ecosystem for consent-based financial data sharing, consent artefact storage, and lifecycle management.
- ✧ Document Management System (DMS): Integration to identify, tag, and manage personal data within documents, link consent artefacts, and enforce retention and deletion policies.
- ✧ HRMS & Internal Systems: Integration with HRMS and internal applications to manage employee personal data in compliance with DPDP Act obligations.
- ✧ Third-Party Service Providers: Integration with vendors, fintech partners, and outsourced service providers for monitoring data sharing, consent enforcement, and compliance tracking.
- ✧ National & State APIs: Integration with relevant Government of India and Kerala State APIs, portals, and digital public infrastructure as applicable, ensuring secure and compliant data exchange
- ✧ Regulatory & Reporting Interfaces: Support for integration with regulatory reporting, audit systems, and incident reporting workflows as mandated under DPDP Act and related directions.

3.4 Security & Compliance Scope in brief

- ✧ Deployment of the DPCMS strictly within Bank-approved infrastructure (Banks DC/DR or Meity-empanelled cloud), in accordance with bank's policies and regulatory hosting guidelines and aligned to DPDP act 2023.

- ✧ Implementation of defence-in-depth security controls, including perimeter security, application security, database security, and operating system hardening.
- ✧ Encryption of personal data at rest and in transit using industry-standard cryptographic algorithms approved by the Bank.
- ✧ Implementation of role-based access control (RBAC), least-privilege principles, and segregation of duties across system users.

  Enablement of multi-factor authentication (MFA) for privileged and administrative access.
- ✧ Comprehensive audit logging and monitoring of user activity, data access, consent events, and system changes, with tamper-evident logs.
- ✧ Integration with Bank / SDC Security Operations Centre (SOC), SIEM, and monitoring tools for real-time security visibility.
- ✧ Support for Vulnerability Assessment and Penetration Testing (VAPT) prior to go-live and at periodic intervals as mandated by the Bank.
- ✧ Compliance with RBI Cyber Security Framework, NABARD IT & Cyber Security advisories, CERT-In directions, and applicable Government of India security guidelines.
- ✧ Secure backup, recovery, and disaster recovery (DR) mechanisms aligned to SDC DR architecture and Bank-approved RTO / RPO.
- ✧ Support for security audits, regulatory inspections, and third-party assessments, including timely closure of observations.

3.5 Data Localisation & Access Control Scope in brief

- ✧ The Bidder must include the details of all hardware and network infrastructure components necessary to implement and maintain the solution for the full contract period, for Storage, processing, and management of all personal data strictly within India with details to be provided in the Technical Proposal. Kerala Bank may provision these components through its DC/DR facilities or an alternate environment; otherwise, the Bidder shall provision them via a Meity-empanelled cloud solution.Explicit prohibition on storage, processing, replication, or backup of Bank data outside India or outside Bank-approved infrastructure.
- ✧ Full data ownership retained by the Bank, including all personal data, consent artefacts, logs, configurations, and reports.
- ✧ Controlled and auditable vendor access, restricted to authorised personnel and provided only with

explicit approval from the Bank.

- ✧ Prohibition on remote access to production systems from outside India without prior written authorisation and secure access mechanisms.
- ✧ Implementation of privileged access management (PAM) controls for administrator and support accounts.
- ✧ Segregation of environments (development, testing, staging, production) with no real personal data used outside production unless explicitly approved.

  Enforced purpose limitation and access control policies ensuring data access strictly on a need-to-know basis.
- ✧ Configurable data retention, archival, and secure deletion controls aligned with DPDP Act, regulatory, and business requirements.
- ✧ Secure handling of logs, backups, and archives, ensuring localisation, encryption, and access traceability. Immediate revocation of access upon change in role, contract termination, or vendor disengagement.

4. **Deliverables**

- ✧ Submission of detailed project plan, governance structure, risk register, and implementation methodology, followed by formal project kick-off meeting.
- ✧ Solution Design & Architecture: Delivery of detailed functional, technical, and security architecture documents aligned to DPDP Act requirements infra hosting requirements as per guidelines.
- ✧ Coordination with the Bank and its infrastructure teams, or self-managed by the bidder as applicable, for provisioning, sizing, configuration, and security hardening of compute, network, and storage resources, for deployment either at the Bank's DC/DR or on MeitY-empanelled cloud platforms.
- ✧ Software Installation & Configuration: Installation of DPCMS software components, configuration of core modules, workflows, roles, and access controls.
- ✧ Integration Deliverables: Completion of integrations with CBS, digital banking channels, DMS, NPCI systems, Aadhaar, DigiLocker, Account Aggregator framework, and other identified systems.
- ✧ Data Discovery & Classification Output: Delivery of initial data discovery results, data classification reports, and data flow mappings across Bank systems.
- ✧ Consent Management Enablement: Configuration and activation of consent capture, lifecycle management, withdrawal mechanisms, and audit artefact storage.
- ✧ Data Principal Rights Workflows: Deployment of end-to-end workflows for access, correction, erasure,

grievance redressal, and SLA tracking.

- ✧ Privacy Governance & Compliance Artefacts: Delivery of Records of Processing Activities (RoPA), policy mappings, retention schedules, and compliance dashboards.
- ✧ Security Hardening & Testing: Completion of security configuration, log enablement, encryption validation, and system hardening activities.
- ✧ VAPT & Security Audit: Conduct of Vulnerability Assessment and Penetration Testing (VAPT) and submission of reports along with remediation and closure of observations.
- ✧ User Acceptance Testing (UAT): Support for UAT including test cases, defect resolution, and formal UAT sign-off by the Bank.
- ✧ Training & Knowledge Transfer: Delivery of role-based training for IT, compliance, audit, and business users, along with user manuals and SOPs.
- ✧ Go-Live & Stabilisation: Production go-live of DPCMS followed by stabilisation support for the contract period.
- ✧ Final Acceptance & Handover: Submission of as-built documentation, source/configuration details (as applicable), asset details, and final acceptance sign-off.
- ✧ The architecture of the proposed solution to be provdied so as to reviewed and approved by the Bank's Information Technology/ Information Security Team. In case any modifications or recommendations are suggested by the IT team, the bidder shall incorporate all such changes during the design phase itself, without impacting project timelines or cost.
- ✧ The solution must be adaptable to accommodate changes in laws, rules, or government policies without requiring architectural overhauls or additional licensing costs. The support for managing these updates/upgrades will be for a period of 5 years from platform Go-live date. Modifications required to meet future statutory or regulatory obligations shall be provided as part of the scope of work and shall not incur additional cost to the Bank.
- ✧ Documentation and support for all updates made to comply with new regulations, including change logs and impact assessments.

5. Eligibility Criteria.

- ✧ Registered startup under Kerala Startup Mission KSUM
- ✧ Demonstrated experience in fintech/regtech, API integration, or AI/ML
- ✧ Prior PoC, pilot, or hackathon experience in financial services preferred.
- ✧ If the proposed solution has not yet been implemented, a POC with the Bank is required.
- ✧ Team with expertise in:

  API aggregation and orchestration AI/ML and NLP

  Cybersecurity and compliance

  UX design for rural/low-literacy users

6. Evaluation Criteria (QCBS 70:30)

Bids are evaluated using QCBS –Quality and Cost Based evaluation method where Quality will be having highest priority and Cost will be the next priority.

STAGE 1: TECHNICAL BIDS EVALUATION [e.g.]

Bidder details	Technical Marks Obtained	Technical Score (TS*)
Bidder1	92 (T1)	(92/92) * 100 = 100
Bidder2	85	(85 / 92) * 100 = 92.39
Bidder3	55	Not applicable
Bidder4	75	(75 / 92) * 100 = 81.52

*Technical score is calculated as TS = (Technical Mark obtained by the bidder / Highest Technical Mark amongst bidders) * 100

The bidders who score 70 marks or above in the technical evaluation will be qualified for Financial Bid evaluation.

STAGE 2: FINAL BID EVALUATION [e.g.]

Bidder details	Financial Bid Amount discovered
Bidder1	1,30,000
Bidder2	1,20,000
Bidder4	1,00,000

Note: The associated infrastructure costs will also be added for the calculation of the Total

Project Cost.

STAGE 3: CONVERSION OF FINANCIAL BID AMOUNT TO SCORE [eg]

Bidder Details	**Financial BidAmount discovered**	**Financial Score (LFB/F*100)**
Bidder1	1,30,000	(100000/130000)*100=76.92
Bidder2	1,20,000	(100000/120000)*100= 83.33
Bidder4	1,00,000 (L1)	(100000/100000)*100 =100

LFB = Lowest Financial Bid from Financial Bid, F = Quoted Amount in Financial Bid

Consolidated Technical & Financial Score (e.g.)

Bidder Details	**Technical Score**	**Financial Score**
Bidder 1	100	76.92
Bidder 2	92.39	83.33
Bidder 4	81.52	100

STAGE 4: COMBINED TECHNICAL AND FINANCIAL SCORE (CTFS)

70:30 weightage for Technical and Financial Score will be used to arrive the Combined Technical and Financial Score (CTFS)

Bidder Details	**Applying weights for the Technical Score & Financial Score**	**CTFS**	**Rank of the Bidder**
Bidder1	100*(70/100) + 76.92*(30/100)= 93.076	93.076	1
Bidder2	92.39*(70/100) + 83.33*(30/100) = 89.672	89.672	2
Bidder4	81.52*(70/100) + 100*(30/100)= 87.064	87.064	3

7. Implementation Timeline

Sl.No	Milestone	Timeline – days
1	Issuance of Purchase Order	T
2	Signing of the agreement, Finalise and signing of implementation Project Plan.	T+1 Month
3	Infrasturucture set up,Insallation &configuration	T+2 months
4	UAT/VAPT	T+2.5 months
5	Go live	T+3 months
6	Stabilisation & Final Acceptance	T + 4 months

8. Proposal Submission Guidelines

- Submit technical and financial proposals when asked for Kerala Startup Mission and for which separate links shall be provided.

9. Terms & Conditions

1. KSCB reserves the right to accept/reject proposals
2. Data privacy and DPDP compliance are mandatory
3. SLAs must define uptime, response times, and support levels
4. Selected vendor must sign an MSA and Non-Disclosure Agreement (NDA).

10. Expansion.

The solution proposed by the bidder should be scalable for expansion. The resource (CPU/ memory / utilization -ensure through system requirment) should not go beyond 70% there should not be any single point of failure in the entire software solution. The entire solution should be configured in high availability mode both at DC and DR with inbuilt redundancy.

So the bidder has to calculate the data growth based on the standard assumption in the industry. This is applicable for all other services which are presently in use and that might get included in future.

11. Infrastructure (Hardware/Network)

The Bidder must include all hardware and network infrastructure components necessary to implement and maintain the solution for the full contract period, with details provided in the Technical Proposal.

Kerala Bank may provision these components through its DC/DR facilities or an alternate environment; otherwise, the Bidder shall provision them via a Meity-empanelled cloud solution.

12. Facility Management Service

The FM support - with minimum two L2 resources should be deployed at Bank's premises, for supporting the solution primarily for 12 hours (viz. 9 am to 7 pm) or as decided by the Bank. However in case of exigency the Bidder shall provide and maintain requisite skilled resources for extended hours as required.

13. Integrity Pact

The Integrity Pact shall be executed by the Bidder, duly stamped and signed on each page, and witnessed by two individuals.

14. Escrow / Similar arrangements

The bidder shall be required to establish and execute an Escrow or equivalent arrangement to ensure that the complete source code, along with all related customization details, is securely deposited with a designated third-party location.

15. Confidentiality

The bidder, by participating in the bidding process, shall regard all document details as strictly confidential. The bidder must undertake that they shall hold in trust any information received by them under the contract /agreement, and the strictest of confidence shall be maintained in respect of such information.

16. Performance & security audit

Performance and security audit of the Data Privacy & Consent Management System (DPCMS) shall be a mandatory activity to ensure the accuracy, availability, integrity, and security of personal data and related systems. The Bank shall appoint a suitable audit firm to conduct performance, security, and compliance audits in accordance with the requirements prescribed by applicable regulators and statutory authorities.

The selected bidder shall extend full cooperation and furnish all information, documentation, system access (as permitted), configurations, logs, and other inputs as required by the audit firm, in the format and manner prescribed by the Bank or the appointed auditor.

All observations, vulnerabilities, non-compliances, and performance issues identified during the audit shall be remediated by the selected bidder within the timelines specified by the Bank, and such remediation shall be completed at no additional cost to the Bank. Successful closure of audit observations to the satisfaction of the Bank shall be a prerequisite for final acceptance and continued operation of the DPCMS.

17. Penalty

The successful bidder shall strictly adhere to the delivery milestones and timelines specified for the implementation of the Data Privacy & Consent Management System (DPCMS). Any failure to meet the agreed implementation schedule, except where such delay is solely attributable to the Bank, shall be treated as a material breach of contractual obligations.

To ensure timely implementation, the Bank reserves the right to levy penalties or liquidated damages for delays attributable to the successful bidder, in accordance with the terms of the contract, without prejudice to any other rights or remedies available to the Bank.

18. Contract Period

5 years.

19. Annexures

Annexure I
Functional requirements

The form has to be filled in all respects.Each raw under subtitles are treated as requirements .

The response shall be given as readily Available (RA) /customisable (CA) and Not Possible (NA) against each numbered row . If any raw is left blank it will be categorized as “Not Possible” for evaluation purpose.

#		Description	RA	CA	NA
1		**Universal Consent Management**			
	A.	**Consent Management Platform**			
	1	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.			
	2	The consent management platform should be able connect to the national consent stack as and when the same is released by Government of India.			
	3	Provide mechanisms for granular consent at the Unique Customer Identification Code / Customer ID level, ensuring purpose specific consent management as per DPDPA 2023.			
	4	Consent collection in the platform should support all three modes of Personal Information input Digital, Physical that is digitized subsequently, through third party agencies collected in physical / digital format.			
	5	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			
	6	Proposed solution shall enable users to set granular preferences for purposes as per requirements determined by business/operation.			
	7	Support for incorporating consent templates based on business requirements.			
	8	Implement mechanisms for obtaining digitally verifiable Parental/ Guardian consent for minors as per the DPDP Act.			
	9	Implement mechanism for obtaining digitally verifiable consent from Persons with Disability (PwDs) and illiterates.			
	10	Design, collect and manage consents as per DPDP Act, 2023 and other relevant regulatory requirements e.g. Reserve Bank of India (RBI), Insurance Regulatory & Development Authority of India (IRDAI), Unique Identification Authority of India (UIDAI), etc.			
	11	Support for hierarchical consent structures based on purposes and user attributes.			
	12	Consent record with timestamp, purpose, and data shared.			
	13	Consent revocation tracking and enforcement.			
	14	Automated consent lifecycle management, from collection, storage, renewal, revocation, logs, security (immutability), and auditability.			

#		Description	RA	CA	NA
	15	Centralized repository for managing user consents.			
	16	Maintain an audit trail of consent records, including timestamps, purposes, and associated processing activities as required under DPDP Act 2023.			
	17	Ensure that consent artefacts are immutable, admissible in court, and meet regulatory standards as per MeitY's Electronic Consent Framework.			
	18	Implement consent retention and expiration mechanisms as per legal and regulatory requirements			
	19	Maintainability of consent nominations similar to RBI nomination norms.			
	20	Maintain consent versions with date and time stamp.			
	21	Consent revaluation after a defined period of time to keep it relevant.			
	22	Trigger necessary communications (Email/ SMS/ Whatsapp / in-app) for expired/expiring consent.			
	23	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.			
	B.	**Integration**			
	1	Integrate seamlessly with third-party systems/ Consent Management Platform as per DPDPA 2023/ UIDAI/ Digi Locker/ IRDAI/ any other platform mandated by Government of India or other Statutory Bodies to centralize consent records and ensure consistency across platforms.			
	2	Maintain a centralized repository for consents collected via third-party platforms.			
	3	Enable syncing of updated consent records with internal and external systems.			
	4	Platform 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.			
	5	Implement robust security measures such as encryption, access controls, and secure data handling practices to protect consent artefacts/ user data.			
	6	The solution should be scalable to handle increasing volumes of consent data as the organization grows.			
	7	Provide an intuitive interface for users to easily manage their consent preferences.			

#		Description	RA	CA	NA
	8	Ensure clear and transparent communication with users regarding their consent choices and data usage.			
2		**Cookie Consent**			
	A	**Cookie scanning and categorization**			
	1	Auto-Scanning of sub-folders and sub-domains of the website and identifying the cookie type for classification as per regulatory requirements (example - Auto-categorization of cookies into essential, functional, analytics, marketing and performance)			
	2	Auto-blocking of cookies, including 3rd party scripts and tags, based on consent provided by the user			
	B	**Cookie Banner**			
	1	Customizable banner template.			
	2	Auto-translation of cookie banner content into 22 languages as mandated by the DPDP Act.			
	C	**Integration with Google Tag Manager**			
	1	Interactive Advertising Bureau's Transparency and Consent Framework compliant cookie banner.			
3		**Data mapping Automation**			
	1	Automated mapping of data processing activities to purpose, legal basis, data category, retention period, and system of record.			
4		**Integration (Structured Data)**			
		The bidder shall ensure that the proposed solution is fully compatible and capable of seamless integration with the existing system or any similar applications being implemented. The integration must support the following			
	1	**Metadata Interoperability:** The solution shall enable ingestion, synchronization, and exchange of metadata using standard interfaces, APIs, or connectors.			
	2	**Governance Alignment:** The solution must preserve and align with existing data governance structures, including data lineage, classifications, stewardship roles, and business glossaries maintained within the EDC.			
	3	**Operational Continuity**: Integration must not disrupt current EDC operations. The solution should support real-time or scheduled metadata updates and ensure continuity of data catalog services.			
	4	**Documentation and Approach:** The bidder shall provide detailed documentation outlining the technical approach for integration, including any dependencies, customization requirements, and limitations.			

#		Description	RA	CA	NA
	5	**Compliance and Standards:** The integration must adhere to industry best practices and standards for metadata management, data governance, and interoperability			
5		**Data Principal Rights Management**			
	A	**Rights Management & Request Handling**			
	1	User friendly Portal for Data principals to view and manage their consents			
	2	Data Principals should be able to download a copy of their consent history.			
	3	Enable mechanisms for Data Principals to raise requests under all rights			
		encapsulated in 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			
		Right to Nominate (in the event of death or Incapacity,Allow to Nominate,modify or revoke a nominee,enable nominees to access withdraw, erase etc.			
	4	Ensure clear and transparent communication with Data Principals throughout the request process.			
	5	Life cycle from invitation to closure.			
	B	**Workflow Automation & Compliance Adherence**			
	1	Implement workflows at the Bank to receive, verify, respond to, and process these requests efficiently.			
	2	Orchestration of SMS / Email/ Whatsapp/ in-app notifications to Data Principals via communication gateways/ Mobile Banking/ Internet Banking.			
	3	Ensure view consent and revoke consent request could be handled in a self- serve manner to reduce number of tickets to be handled by privacy team or DPO office			
	4	Workflow management should be configurable to streamline the entire process from intake till fulfillment			
	5	Seamless integration with existing systems and data sources to facilitate efficient data discovery and retrieval.			
	C	**Integration & Multi-Level Workflow Capabilities and Data Discovery Outcomes**			

#		Description	RA	CA	NA
	1	Orchestrate data deletion requests between the Data Fiduciary and the Data Processors. Enable the service agents to verify consent artefacts and discover personal data relating to the deletion request and take appropriate action			
	D	**Tracking, Reporting & Auditability**			
	1	Maintain a centralized register/ tracker to record all Data Principal Requests, responses, and resolution times, demonstrating compliance			
	2	Securely log and track all requests to enable verification, audits, and regulatory reporting.			
6		**Privacy Assessment**			
	A	**Core Privacy Assessment Features**			
	1	Privacy Impact Assessments (PIAs):			
		- Automated workflows for conducting PIAs			
		- Built-in templates aligned with DPDPA			
		- Risk scoring and mitigation recommendations.			
		- Integration with data maps and business processes.			
	2	Data Discovery & Classification:			
		- AI/ML-powered scanning of structured and unstructured data.			
		- Identification of sensitive personal data across systems.			
		- Risk-based categorization and tagging.			
	3	Assessment Assignment & Response Tracking:			
		- Ability to assign assessments to projects or data assets.			
		- Role-based access for stakeholders to complete and review assessments.			
		- Audit trails and exportable reports.			
	4	Customizable Assessment Templates:			
		Create assessments tailored to specific data uses or business units.			
		- Modify built-in templates to suit organizational needs.			
		- Support for multilingual and region-specific compliance.			
		- Compliance & Risk Management Features			
	5	Consent Management Integration			
		- Track and manage user consent across platforms.			
		- Ensure lawful data collection and processing.			
		- Real-time updates for regional compliance			
	6	Vendor Risk Management:			

#		Description	RA	CA	NA
		- Assess third-party compliance posture.			
		- Automate vendor assessments and reporting.			
		- Maintain records of vendor data handling practices.			
	7	Incident & Breach Management:			
		- Real-time alerts and breach notification workflows			
		- Regulatory reporting templates.			
		- Post-incident analysis and remediation tracking.			
	B	**Operational & Strategic Features**			
	1	Role-Based Access & Governance: ● Define roles like Privacy Curator, Data Curator, Privacy Reader. ● Control who can create, edit, approve, or view assessments.			
	2	Automated Compliance Workflows: ● Trigger assessments based on privacy rules or data conditions. ● Integration with CRM, ERP, core banking application and data governance platforms. ● Continuous monitoring and compliance scoring.			
	3	Reporting & Analytics: ● Dashboards for privacy metrics and compliance status. ● Exportable reports for audits and board-level reviews. ● Benchmarking against industry standards			
7		**Data Protection Impact Assessments**			
	A	**Comprehensive DPIA Templates & Workflows**			
	1	Provide standardized templates and workflows for conducting DPIAs, covering			
	1.1	Description of processing activities, including involvement of third parties			
	1.2	Risk assessment matrix to evaluate risks and automated risk calculation & categorization of all products/ process wise.			
	1.3	Regulatory and industry specific DPIA templates, customizable as per business needs.			
	1.4	Automation & Workflow Management			
	1.5	Enable multi-level workflow capability to facilitate role-based access, permissions, and approvals.			
	1.6	Allow customization of roles, permissions, and review processes to align with organizational structures.			
	1.7	Support auto-reminders, query escalation, and follow-ups to streamline DPIA completion.			
	1.8	Provide the ability to upload supporting documents and artefacts when responding to specific queries.			

#		Description	RA	CA	NA
	1.9	Periodic & Proactive Assessments			
	1.10	Support periodic DPIA reviews to ensure ongoing compliance with regulatory requir1ements.			
	1.11	Proactively launch assessments for new business processes, with a timeline view for accountability and visibility.			
	1.12	Collaboration & Vendor Engagement			
	1.13	Enable seamless sharing of DPIA assessments with data processors and vendors, ensuring end-to-end compliance.			
	1.14	Provide functionality to add team members and external stakeholders for collaborative assessments			
	1.15	Smart Assessments			
	1.16	Auto-fill assessments using AI leveraging knowledge base of consent artefacts, processors, configurations and data discovery findings.			
	2	Controls, Reporting and Dashboard			
	2.1	Real Time Monitoring: Dashboard should provide real time visibility into the initiation, review, approval and closure of DPIAs across all Branches and Business functions			
	2.2	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.			
	2.3	Alerts and Escalations: Support for automated alerts and escalations to DPOs, Privacy Stewards, or relevant functionaries in case of SLA breaches or pending approvals.			
	2.4	Branch Wise & Function Wise Compliance Overview: Ability to generate compliance scorecards and dashboards for each branch, Region, Zone, Department or business Vertical.			
	2.5	Role-Based Access Controls (RBAC): The system should allow differentiated access for			
	2.6	DPO – Global access with configuration and oversight privileges			
	2.7	Privacy Stewards – Access to DPIAs within their assigned branches/Verticals			
	2.8	Branch/Region/Zone – Access to DPIAs initiated or owned by their teams			
	2.9	The platform must be scalable to onboard all branches and new privacy stakeholders as per future organizational requirements.			

#		Description	RA	CA	NA
8		**Privacy Notice Management**			
	A	**Notice & Transparency Mechanisms**			
	1	Ability to generate customizable & dynamic notices tailored to different products and journeys.			
	2	Provide downloadable 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	Provide banking options (logos & themes) to relate with the Bank's design language.			
	B	**Version control**			
	1	Maintain version control for all notices generated within the user journey.			
	2	Record and store multiple versions of consent agreements and maintain historical consent changes for audits.			
	C	**Audit & Reporting**			
	1	Audit trail for all consent related activities and same cannot be altered.			
	2	Ensure identification and notification to Data Principals who consented to outdated versions.			
9		**Data Breach Management**			
	A	**Regulatory Reporting & Compliance**			
	1	Breach reporting mechanism to be in place/facilitated.			
	2	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.			
	3	Maintains a repository of pre-approved templates for quick and compliant breach reporting.			
	4	Show steps taken to contain the breach, demonstrating transparency and trust.			
	B	**Final Communication & Documentation**			
	1	Send initial and final breach reports to both impacted Data Principals and Data Protection Board.			
	2	Maintain an audit trail of all breach-related actions for demonstration of compliance.			
	C	**Bulk Breach Notifications**			
	1	Create cohorts of Data Principals to ensure that the notification is only going out to the affected Data Principals.			
	2	Automated breach notices sent to impacted Data Principals within the timeframe as defined by DPDPA Act and rules.			

#		Description	RA	CA	NA
	3	Configurable templates for breach intimation, ensuring compliance and clarity.			
	4	Suggest remedies to impacted Data Principals to mitigate risks.			
	5	Show steps taken to contain the breach, ensuring transparency and trust.			
	6	Integration with existing SOC and SIEM platform/Regulatory agencies for reporting			
10		**Privacy by Design**			
	1	To provide internal teams with an end-to-end mechanism for identifying personal data related changes in applications and processes and raise a Privacy by Design (PbD) request that can be evaluated, managed and monitored by the Bank's privacy team as per Privacy by Design (PbD) principles			
11		**Training and Knowledge Transfer**			
	1	Provide training (technical & functional) & documentation to relevant business teams of the Bank and personnel on the implemented Consent Management and Data Privacy use cases for each aforementioned module			
12		**Testing and Validation**			
	1	Test cases to be prepared by bidder and to capture the testing artifacts and share it with the Bank.			
	2	Conduct performance testing of tool.			
	3	Test the integration of the tool with critical applications, including version control systems, build systems, and issue tracking tools.			
	4	Work with business teams to execute UAT for all integrations and releases.			
13		**Reporting and Metrics**			
	1	Set up reporting mechanisms to track key performance indicators (KPIs) and security metrics.			
	2	Generate and distribute reports to relevant stake holdersas per requirement of the Bank and statutory compliance .			
14		**Security requirements**			
	1	The tool should support standard authentication with AD / SOS			
	2	Support different authentication methods for different populations of users.			
	3	Solution should be accessible from any network, but should allow restricting access to a definable corporate network range for specific populations of users.			
	4	Connection/Transmission to the on-prem applications should be over encrypted channel.			
	5	All confidential information such as passwords, Security Questions/Information should be over secured encrypted channel.			

#		Description	RA	CA	NA
15		**Compliance and Governance**			
	1	Ensure that the tool aligns with industry standards and regulatory requirements stated in India DPDPA.Implementation of governance model.			
16		**Research Repository on Data Protection Laws**			
	1	The bidder shall develop and maintain a secure and user-friendly Research Repository focused on Indian data protection laws, including the Digital Personal Data Protection Act, 2023, Digital Personal Data Protection Rules 2025, Information Technology Act, 2000, Information technology (Amendment) Act 2008, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011			
	2	The repository should also support international data protection laws, industry best practices, new laws enacted globally and any amendments to the existing laws/ rules.			
17		**Additional Scope of Work**			
	1	Proposed Solution shall support explicit, implicit, opt-in, and opt-out consent models.			
	2	Proposed Solution shall have capabilities for integration with existing systems of the Banks current technology stack and eco-system (Mobile Banking, Internet Banking, CRM, various journey initiated by Bank etc.) API or other suitable technologies shall be used for seamless integration with internal and third-party systems or other secure integration as agreed by the Bank.			
	3	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.			
	4	Proposed Solution shall have Customizable consent forms like Branding options (logos, themes), Dynamic content based on user location or preferences etc.			
	5	Proposed Solution shall support versioning to track changes in consent forms.			
	6	Proposed Solution shall record and store multiple versions of consent agreements and maintain historical consent changes for audits.			
	7	Proposed Solution shall have Audit trails for all consent-related activities and same cannot be altered. Integrity to be ensured for the same. Further, Detailed logs of consent-related activities to be available in a user-friendly interface customized to regulatory requirement for audits.			
	8	Proposed Solution shall have feature for Real-time consent updates and synchronization across systems.			
	9	Proposed Solution shall support for hierarchical consent structures like consent for specific data types or purposes etc.			

#		Description	RA	CA	NA
	10	Bidder shall provide SBOM & CBOM (Software Bill of Material and Cryptographic Bill of material) of proposed solution to the bank.			
	11	Proposed Solution shall have Centralized repository for managing user consents			
	12	Proposed Solution shall have dashboard for end-users to view and manage their consents, Download a copy of their consent history,			
	13	Proposed solution shall enable users to set granular preferences like data sharing, marketing communications etc.			
	14	Proposed Solution shall support for self-service consent revocation.			
	15	Proposed Solution shall have feature for Real-time reporting on consent metrics like consent rates, revocation trends, Geographic distribution of consents etc.			
	16	Proposed Solution shall have automated consent expiration and renewal workflows.			
	17	Proposed Solution shall have ability to handle large user bases and high transaction volumes.			
	18	Proposed Solution shall have Low-latency operations for real-time consent capture and verification.			
	19	Proposed Solution shall have Role-based access controls to to manage internal access.			
	20	Proposed Solution shall have Data encryption (at rest and in transit).			
	21	Proposed Solution shall have feature for secure deletion of consent records upon user request or expiry.			
	22	Proposed Solution shall have feature for Data masking and anonymization for non-essential records.			
	23	Proposed Solution shall have built-in feature for compliance with major data privacy laws.			
	24	Proposed Solution shall provide regular security updates and patches.			
	25	Proposed Solution shall have feature for Real-time system health dashboards.			
	26	Proposed Solution shall have feature for alerts for failures, latency issues, or integration errors.			
	27	The proposed platform should have ticketing mechanism to address the issues/ queries raised by the Bank users.			
	28	The bidder shall execute escrow agreement for source code for the consent management application without any cost to Bank.			

#		Description	RA	CA	NA
	29	The solution should support DC/DR integration and periodic DR drill execution as per the Bank's IT/BCP policy.			
	30	The solution must support data migration to cloud platforms , if required by the Bank. It should comply with applicable data protection regulations, including data residency, encryption standards, and access controls.			
	31	The solution must have ability to support real time replication through dedicated private connect capability from the service provider's Cloud SaaS to Bank's DC and DR/ Nr DR.			
	32	The solution must have ability to support access for Bank users through a dedicated private connect capability from Bank's gateway to their Cloud SaaS application			
	33	The system must have the capability to adapt to any future regulatory requirements issued by DPBI/ MeitY/ RBI or any Regulatory Agencies under the DPDP Act, 2023 or any relevant Act/ Rules.			
	34	Bidder has to provide Source Code review report of proposed application with compliance validation from Cert-IN empaneled audit organization to Bank annually without any cost to Bank.			
	35	The proposed solution should support Customer Managed Key (CMK) or Bring Your Own Key (BYOK) to provide control to the Bank.			
	36	The selected Bidder shall closely work with any Consultant(s)/ Advisor (s) appointed by the Bank for the purpose of this engagement. This includes, but is not limited to, participating in joint discussions, sharing relevant documentation, aligning on project timelines and deliverables, and incorporating feedback or recommendations provided by the Consultant(s) as directed by the Bank.			
	37	The Bidder shall ensure that its team is available for coordination meetings, workshops, and review sessions as scheduled by the Principal or its Consultant(s). The Bidder shall also provide timely responses to queries and inputs sought by the Consultant(s) to facilitate effective project execution.			
	38	All such association shall be undertaken in a professional and cooperative manner, with the objective of achieving the Banks strategic and compliance goals. The Consultant(s)/ Advisor(s) shall not be construed as having any authority over the Bidder, except as explicitly communicated by the Bank.			

Annexure II – Technical requirements

The form has to be filled in all respects. If any raw is left blank it will be categorized as "Not Possible" for evaluation purpose.

Sl#	Description	Readily Available (RA)	Customisable (CA)	Not Available (NA)
1	The selected vendor should host the solution in High Availability mode, with DR and a minimum uptime time of 99%.			
2	Encryption at rest. In use & in transit			
3	Secure API integrations			
4	Audit logs and SIEM integration			

5	Data localisation compliance			
6	Role-based access control			
7	Production, Pre production, DR , Training ,Development&UAT environments.			
8	Rregulatory /statutory guidelines / requirement free of cost to the Bank during the contract period.			
9	Proactive monitoring and capacity planning well in advance at regular intervals and advise the Bank on software/hardware upgrades.			

Annexure III - API Aggregator- integration details

Sl#	Service	Facilities	Aggregator Name
1			
2			
3			
4			
5			

Bidder can add more rows to mention the API aggregator details.

Annexure IV – Details of Proposed Network components

Serial Number	Item Description	Make C Model	Version/Specification	Capacity such as number of ports/connections	No of License/users	Warranty Period	Support Details	Any other information

Annexure V – Details of Proposed Hardware Infrastructure

Serial Number	Make C Model	Processor Type C clock speed	Number of cores per server	Total Memory per server	Hard Disk typeC capacity etc. per server	RAID Particulars per server	Operating System per server	Redundant Network bandwidth per server	Redundant Power Supply (RPS)	Number of Physical servers	Other particulars .	whether deployed in VM /shared	Function / purpose

Annexure VI - Declarations

- Eligibility Declaration
- Conflict of Interest Declaration
- NDA Acceptance
- Integrity Pact
- Details of Existing Installations.