

THE KHAMGAON URBAN CO-OPERATIVE BANK LTD.

Multi-State Scheduled Bank | Head Office: Khamgaon, Dist. Buldhana

TENDER / RFP

DPDP Act Implementation and Privacy / Consent Management Solution

INVITATION OF PROPOSALS FOR DPDP ACT IMPLEMENTATION AND PRIVACY / CONSENT MANAGEMENT SOLUTION

Tender Reference	KUCB/RFP/DPDP-CMS/2026-27/003
RFP Issue Date	08 October 2026
Last date and time for submission	20 October 2026, 11:59 PM IST
Proposal validity	90 days from the last date of submission, unless amended by the Bank
Contract period	Three (3) years from commencement/go-live, with extension only by written agreement
Submission email IDs	dadhich@khamgaonurban.bank.in; rushibhalerao@khamgaonurban.bank.in
CC	santoshjadhao@khamgaonurban.bank.in; prabhakarpatil@khamgaonurban.bank.in
Email subject	Proposal for DPDP Implementation and Privacy / Consent Management Solution

1. Invitation

The Khamgaon Urban Co-operative Bank Ltd. ("the Bank") invites proposals from eligible and experienced technology providers / implementation partners for assessment, design, supply, configuration, implementation, integration, training, support and maintenance of a DPDP implementation and Privacy / Consent Management Solution for an initial period of three (3) years. The solution may be deployed on-premises or on cloud, subject to the Bank's security, data-residency, regulatory, procurement and approval requirements.

The solution and services shall support the Digital Personal Data Protection Act, 2023, the Digital Personal Data Protection Rules, 2025, relevant amendments/corrigenda, and other applicable legal and regulatory requirements, to the extent in force and applicable from time to time. The bidder shall provide a provision-wise applicability and commencement tracker and shall support the Bank in updating its controls as requirements change.

2. Objectives and scope

The engagement is intended to help the Bank establish and maintain a documented privacy governance framework and operational workflows, supported by technology. The bidder shall perform discovery and gap assessment, recommend a prioritised implementation roadmap, configure or develop the solution, integrate agreed systems, test the workflows, train users and provide post-implementation support. The bidder shall identify assumptions, dependencies, exclusions, third-party requirements and items requiring Bank decisions.

Phase 1 — Data discovery, inventory and lifecycle governance

Identify and maintain an inventory of personal data and processing activities across CBS, customer and loan systems, digital banking, databases, file shares, email, endpoints, cloud/SaaS and relevant third parties, as applicable. Document data categories, purposes, owners/custodians, locations, recipients/processors, data flows, retention rules, deletion, archival and legal-hold requirements. Provide discovery methodology, coverage limitations and a gap register.

Phase 2 — Data Principal rights and grievance redressal

Provide configurable workflows for receiving, identity verification, assignment, tracking, response, escalation and closure of applicable requests, including access, correction, completion/updating, erasure, nomination and grievance redressal, as applicable under law. Maintain timestamps, responsibility, communications, exceptions and auditable evidence. Consent withdrawal shall be supported where relevant.

Phase 3 — Privacy notices, purpose and consent management

Create and version privacy notices in clear language; capture consent records with purpose, notice version, timestamp, channel/source and relevant evidence; maintain consent history; support renewal, modification and withdrawal; and propagate changes to connected systems where technically feasible. Record the applicable lawful ground and supporting information where consent is not the relevant basis. The Bank shall approve legal wording and purposes before production use.

Phase 4 — Security safeguards and personal data breach support

Support role-based access, least privilege, administrator controls, multi-factor authentication where supported, encryption in transit and at rest, access logging, monitoring, retention enforcement, backup/recovery and integration with the Bank's existing security controls. Provide incident logging, escalation, investigation support, evidence preservation, corrective action tracking and assistance with breach communications/reporting within timelines specified by applicable law and the Bank's policy.

Phase 5 — Governance, accountability, audit and continuous compliance

Maintain policy/procedure registers, processing and consent records, audit trails, evidence repository, exception and remediation registers, privacy risk assessments where applicable, third-party/processor oversight, training records, management dashboards and periodic compliance reports. Provide audit-ready exports and support internal, external and regulatory reviews.

3. Minimum functional, technical and security requirements

- **Integration:** Supported APIs/connectors or documented interfaces for CBS and other agreed Bank systems. The bidder shall submit an interface inventory, architecture, data-flow diagrams, prerequisites, dependencies, error handling, reconciliation and integration limitations. No interface is deemed included unless expressly identified in the proposal and contract.
- **Deployment and data residency:** Disclose deployment model, primary and DR locations, data flows, backup locations, support locations, subprocessors and any remote access. Bank/personal data must remain in India. No transfer, remote access from outside India, or change of hosting/subprocessor/location without prior written Bank approval and compliance with applicable requirements.
- **Identity and access:** Role-based access, least privilege, maker-checker/dual control for sensitive administration where appropriate, MFA for privileged access, unique user IDs, periodic access review and timely revocation.
- **Logging and monitoring:** Tamper-evident audit logs for access, administrative activity, consent/notice changes, rights requests, exports, deletion and configuration changes. Specify log retention, search/export capability, time synchronisation and integration with Bank monitoring tools where applicable.
- **Encryption and key management:** Encryption in transit and at rest, key ownership/location, rotation and access controls. Clearly state any exceptions and compensating controls.
- **Secure development and vulnerability management:** Secure SDLC, dependency and component inventory where applicable, vulnerability assessment/penetration testing, remediation SLAs, patch management and disclosure of material security incidents affecting the solution.
- **Resilience:** Document backup frequency, retention, restoration testing, DR architecture, RPO/RTO commitments and service availability. Propose measurable SLAs and service credits for approval by the Bank.
- **Incident management:** Notify the Bank of any actual or suspected incident affecting Bank data or services without undue delay and within the shorter of the contractually agreed timeline or applicable legal/regulatory timeline. Provide a 24x7 escalation contact, updates, root-cause analysis and corrective/preventive actions.
- **Data minimisation and testing:** Use synthetic or masked data for demonstrations, testing and POC unless the Bank gives prior written approval for another approach. Production data shall not be copied to vendor environments without documented approval and safeguards.

- Exit and portability: Provide complete export of Bank data, configurations, notices, consent records, logs and evidence in commonly usable formats, together with data dictionary and transition assistance. On exit, return or securely delete Bank data and provide a deletion certificate, subject to legal retention obligations.
- Reporting: Consent and withdrawal status; rights requests and ageing; inventory and lifecycle status; incidents; exceptions and remediation; audit logs; third-party status; SLA performance; and overall implementation/compliance progress.
- Accessibility and usability: Provide clear user workflows, searchable records, configurable roles, usable reports and documentation. Identify supported browsers, languages, capacity limits and product dependencies.

4. Implementation deliverables and acceptance

- Project initiation document, governance structure, detailed work plan, milestone schedule, RACI matrix and risk/issue/dependency register.
- Current-state discovery and gap assessment, data inventory, data-flow diagrams, prioritised remediation roadmap and provision-wise legal applicability tracker.
- Solution architecture, security design, hosting/data-residency declaration, integration specifications, interface inventory and configuration documentation.
- Configured workflows for notices, consent, rights requests, grievance handling, incidents, retention/lifecycle and governance reporting as applicable.
- Test strategy, test cases, test results, defect register, security test reports, UAT support and written Bank acceptance before production go-live.
- Administrator and user manuals, SOPs, training material, knowledge-transfer sessions and attendance/competency records.
- Go-live plan, rollback plan, hypercare support, periodic service reports and agreed operational runbooks.
- Exit plan, data export procedure, secure deletion process and transition assistance.

Deliverables shall be accepted only after review against agreed acceptance criteria. Payment shall be linked to milestones and written acceptance, not merely to submission of documents or completion of vendor activities. The Bank may require correction and resubmission of deficient deliverables at no additional cost where they fail to meet the agreed specifications.

5. Service levels and support

Bidders shall propose service availability, support hours, severity definitions, response and resolution targets, escalation levels, planned-maintenance windows, backup/restore commitments, DR objectives, service reporting and service credits. The final SLA shall be agreed before award. The bidder shall disclose support staffing, location, subcontractors and arrangements for continuity of service. The Bank may specify stricter requirements during contract finalisation.

6. Bidder eligibility and documents

- Certificate of incorporation/registration, PAN, GST registration and authorised signatory details.
- Relevant experience in privacy/data protection, data governance, consent management, data discovery, security or comparable implementation services; banking/BFSI experience and at least three client references are preferred.
- Product/OEM authorisation, if applicable; details of ownership, product name/version, licensing model and material third-party dependencies.
- Audited financial statements for the last three financial years and a CA-certified average annual turnover statement. Recommended criterion for Bank approval: average annual turnover of at least ₹3 crore over the last three audited financial years. The Bank may revise this threshold before publication based on procurement policy and market assessment.
- Proposed architecture and deployment model; India data-residency undertaking; list of data locations, subprocessors and support locations.
- Implementation methodology, timeline, staffing plan, support/escalation model, proposed SLA and business continuity arrangements.

- Security certifications and independent audit/test reports, where available; details of material security incidents, litigation or debarment that the bidder is required to disclose under applicable procurement policy.
- Completed requirement-wise compliance matrix marked Comply / Partially Comply / Do Not Comply, with evidence, remarks, assumptions and deviations.
- Separate list of exclusions, additional costs, required Bank dependencies and items requiring third-party procurement.

7. Commercial proposal

Quote itemised costs in INR, excluding and including applicable taxes, for:

- Software licence/subscription and user/volume bands;
- Discovery, assessment and implementation;
- Configuration/customisation and integrations, itemised by interface;
- Data inventory, classification, migration or cleansing, if applicable;
- Training, documentation and knowledge transfer;
- Hosting, backup, DR and other recurring charges;
- Annual support, maintenance, upgrades and version changes;
- Optional services and third-party products;
- Exit, data export and transition assistance; and
- Any travel, out-of-pocket or other charges.

Provide Year 1, Year 2 and Year 3 costs, one-time versus recurring charges, assumptions, taxes, payment milestones, price validity, renewal/extension rates and any price escalation. No unlisted charge shall be payable unless approved in writing by the Bank through the applicable change-control process.

8. Proposal submission and evaluation

Submit signed technical and commercial proposals with supporting documents to the email IDs stated above by the last date/time. Recommended submission method: two separately password-protected files or other method approved by the Bank, with the technical proposal and commercial proposal clearly separated. The Bank shall communicate how and when passwords are to be provided, if this method is adopted. Late or incomplete bids may be rejected under the Bank's policy.

The Bank may evaluate proposals in the following sequence:

1. Preliminary scrutiny of completeness and eligibility documents;
2. Technical evaluation against the published compliance matrix and mandatory requirements;
3. Demonstration, reference checks, clarification or proof of concept, if required;
4. Assessment of implementation plan, security, integration, data residency, support and total cost of ownership; and
5. Commercial evaluation of technically qualified bidders under the Bank's approved procurement method.

The Bank should specify any minimum technical qualifying score and the commercial evaluation formula in the final issued RFP. Evaluation criteria shall not be changed after bid receipt except as permitted by applicable policy and communicated transparently to all affected bidders.

9. Contractual, confidentiality and regulatory conditions

- The selected bidder shall execute a formal agreement, NDA, data-processing agreement, SLA and security schedules before receiving Bank data or commencing production work.
- The Bank shall retain ownership/control of its data, records, configurations and Bank-specific deliverables, subject to clearly stated third-party intellectual-property rights. The bidder shall disclose any restrictions on use, export or transition.
- The bidder shall process Bank data only on documented instructions, for agreed purposes, and shall not sell, reuse, profile, disclose or use it to train models or for product improvement without prior written Bank approval.
- The Bank and its authorised auditors/regulators shall have appropriate audit, inspection and evidence-access rights, subject to applicable law and agreed security protocols.

- The bidder shall obtain prior written approval for subcontractors and remain responsible for their acts/omissions. Subcontractors shall be bound by equivalent confidentiality, security and data-protection obligations.
- The bidder shall support the Bank's incident investigation, regulatory reporting, customer communication and remediation obligations. Contractual timelines shall not delay any statutory or regulatory reporting deadline.
- The contract shall define liability, indemnities, insurance (if required), termination rights, suspension, force majeure, dispute resolution, governing law and business continuity responsibilities.
- The bidder shall not claim that implementation of the solution by itself guarantees compliance. The Bank retains its statutory responsibilities; the bidder is accountable for contracted deliverables and services.
- The Bank reserves the right to seek clarifications, verify submitted information, negotiate where permitted, accept or reject any or all proposals, cancel/reissue the tender or modify the process in accordance with applicable law and Bank policy. Submission does not guarantee award.

10. Bidder declaration

The bidder shall confirm that the information submitted is accurate; all deviations, assumptions, exclusions and third-party dependencies have been disclosed; the bidder has authority to offer the proposed solution; and the bidder will comply with the confidentiality, security, data-residency, audit and contractual obligations agreed with the Bank.

Annexure A — Requirement compliance matrix (to be completed by bidder)

Ref.	Requirement	Status (C/PC/NC)	Evidence / deviation	remarks /
A1	Data discovery, inventory and data-flow mapping			
A2	Notice, purpose and consent lifecycle management			
A3	Data Principal rights and grievance workflow			
A4	Applicable lawful-ground recording where consent is not relevant			
A5	Retention, deletion, archival and legal holds			
A6	Incident and breach-response support			
A7	Access control, MFA, logging and encryption			
A8	India data residency, subprocessor disclosure and remote access controls			
A9	CBS and other system integration / API documentation			
A10	Audit evidence, reports and export			
A11	Backup, recovery, DR and service levels			
A12	Training, documentation, UAT and acceptance			
A13	Exit, data portability, secure deletion and transition			
A14	Implementation timeline, governance and RACI			