



REQUEST FOR PROPOSAL

FOR

PROCUREMENT OF DPDP SUITE AND SELECTION OF SYSTEM INTEGRATOR (SI) CUM CONSULTANT SERVICES FOR SUPPLY, INSTALLATION, INTEGRATION, IMPLEMENTATION AND MANAGEMENT OF DIGITAL PERSONAL DATA PROTECTION SOLUTION FOR A PERIOD OF 3 YEARS

RFP NO: PSB/HO DPO/2026-27/RFP/RG1 DATED 01/10/2026

Address

PUNJAB & SIND BANK

Data Protection Office

Corporate Office, Block 3, NBCC Complex,
East Kidwai Nagar, New Delhi – 110023

TABLE OF CONTENTS

1	KEY INFORMATION	6
2	GLOSSARY	9
3	DISCLAIMER	11
4	INTRODUCTION	12
5	PROJECT OBJECTIVE	12
5.1	Purpose.....	13
6	INSTRUCTIONS TO BIDDERS	14
6.1	Language of the Bid.....	14
6.2	Bid Currency & Price Structure.....	14
6.3	Bid System Offer.....	14
6.4	Two Bid System:	15
6.4.1	Preparation of Bids:	15
6.5	Cost of Preparation	16
6.6	Normalization of Bids.....	16
6.7	Submission of Bid and communication	17
6.8	Late bids	18
6.9	Modifications and/ or Withdrawal of Bids	18
6.10	Earnest Money Deposit (EMD).....	18
6.11	Performance Bank Guarantee/Security Deposit (PBG).....	19
6.12	No commitment to accept lowest or any bid.....	20
6.13	Right to Accept Any Bid and to Reject Any OR All Bids/Cancellation of Tender process	21
6.14	Correction of Errors.....	21
6.15	Soft copy of tender document.....	22
6.16	Bid validity period	22
6.17	Pre-bid meeting	22
6.18	Amendment to RFP Contents	23
6.19	Disqualification	24
6.20	Fixed Price.....	24
6.21	Project Execution	24
6.22	Confidentiality of the Bid Document	24
7	SCOPE OF WORK	24
7.1	System Integrator (SI) cum Consultant — Scope of Work & Responsibilities.....	24
7.1.1	Objectives.....	25
7.1.2	Coverage	25
7.1.3	Consultant (Advisory, Legal & Compliance) Responsibilities	26

7.1.4	System Integrator (Technical Implementation) Responsibilities	29
7.1.5	Compliance of Audit Observations	30
7.1.6	Acceptance and Sign-off	31
7.1.7	Integration Approach & Responsibilities	31
7.2	The DPDP Suite — Detailed Technical & Functional Requirements	32
7.2.1	Notice & Consent Management.....	32
7.2.2	Cookie Management	34
7.2.3	Data Principal Rights Management (DPRM).....	34
7.2.4	Third Party Risk Management	35
7.2.5	Personal Data Discovery & Data Security Posture Managements.....	36
7.2.6	Record of Processing Activities (RoPA)/ Data Protection Impact Assessment (DPIA)	37
7.2.7	Data Breach & Incident Management	39
7.2.8	Privacy Enhancing Technology (Data Encryption, Masking, Tokenization and Anonymization).....	39
7.2.9	Privacy Threat Modelling.....	40
7.2.10	Privacy Training Awareness	40
7.2.11	Dashboards and Reporting, Audit Logs.....	41
7.3	Non- Functional Requirements	41
7.4	Functional and Technical Requirements questionnaire.....	42
7.5	Other requirements	42
7.5.1	Training	44
7.6	Annual Technical Support (ATS)	45
7.7	Resource Requirement.....	46
7.7.1	Roles & Responsibilities.....	48
7.7.2	Duties of Bidder.....	50
7.8	Facilities to be Provided by the Bank	52
7.9	DR Drill.....	52
7.10	DR Setup	52
7.11	System Recovery	52
7.12	Performance and Scalability	53
7.13	Non-Exhaustive Clause	53
7.14	CSITE Undertaking Clause	53
7.15	Exit Plan Management	54
7.16	Security Management.....	56
7.17	Escrow	57
8	CONTRACT PERIOD	58
8.1	End of Sales / End of Support.....	58

8.2	Pre-Contract Integrity Pact.....	59
8.3	SBOM/CBOM:	59
9	PROJECT TIMELINES	59
10	EVALUATION CRITERIA	60
10.1	Preliminary Scrutiny	60
10.2	Eligibility Evaluation Criteria	61
10.3	Evaluation Process	65
10.3.1	Stage 1 — Eligibility and Technical Bid Evaluation	65
10.3.2	Stage 2 - Commercial Evaluation.....	72
10.3.3	Final Evaluation - Weighted Techno Commercial Evaluation Acceptance of Bid & Signing of Contract.....	72
11	PAYMENT TERMS	74
12	SERVICE LEVELS & PENALTIES	76
12.1	Service Level Agreement	76
12.2	Penalties	78
13	TERMS AND CONDITIONS	81
13.1	Assignment & Subcontracting.....	81
13.2	Delays in the Bidder's Performance	82
13.3	Jurisdiction.....	82
13.4	Dispute Resolution.....	82
13.5	Notices	83
13.6	Legal Compliance	83
13.7	DPDP Compliance	83
13.8	Authorized Signatory	85
13.9	Confidentiality.....	85
13.10	Indemnity	86
13.11	Make in India	87
13.12	Force Majeure	87
13.13	Ownership & Retention of Documents:.....	88
13.14	Conflict of Interest.....	89
13.15	Signing of Pre-Contract Integrity Pact:.....	89
13.16	Intellectual Property Indemnity:	89
13.17	Limitation of Liability	89
13.18	Order Cancellation.....	90
13.19	Consequences of Termination.....	92
13.20	Audit by Third Party	93
	APPENDIX	95
	APPENDIX 1: Functional & Technical Compliance Sheet:	95

APPENDIX 2 : Commercial Bill of Materials.....	107
ANNEXURES	
117	
Annexure 1: Submission Checklist (on bidder's letterhead)	117
Annexure 2: Bidder's Information	118
Annexure 3: Tender Covering Letter.....	121
Annexure 4: Bid Security Declaration	123
Annexure 5: Pre-Qualification Criteria	125
Annexure 6: Acceptance/Compliance Certificate.....	126
Annexure 7: Manufacturer's Authorization Form (MAF).....	127
Annexure 8: Escalation Matrix.....	129
Annexure 9: Litigation Certificate.....	130
Annexure 10: Non-blacklisting undertaking	131
Annexure 11: Undertaking of Authenticity (on bidder's letterhead)	132
Annexure 12: Non-Disclosure Agreement	133
Annexure 13: Commercial Proposal Submission Checklist	140
Annexure 14: Bank Guarantee Format for Earnest Money Deposit.....	141
Annexure 15: Format of Performance Guarantee.....	143
Annexure 16 : Pre-contract integrity pact	147
Annexure 17: Compliance with Scope of Work and SBOM	153
Annexure 18: S-BOM & C-BOM details of all the proposed Tool/solutions.....	155
Annexure 19: Minimum Local Content Certification.....	158
Annexure 20 Client References Format	159
Annexure 21: Pre-bid Query format	160
Annexure 22: Proposed Resources CV	161
Annexure 23: Undertaking for Being the OEM/OSD of the Offered Primary Product.....	162

1 KEY INFORMATION

Particulars	Details
RFP Number and Date	RFP NO: PSB/HO DPO/2026-27/RFP/RG1 DATED 01/10/2026
Tender Title	Request for Proposal (RFP) for Procurement of DPDP Suite and selection of System Integrator (SI) cum consultant services for Supply, Installation, Integration, Implementation and Management of Digital Personal Data Protection Solution for a period of 3 Years
Security Deposit/Earnest Money Deposit	Rs.70 lakhs (INR Seventy lakhs only) Note: - Bidders who are eligible for EMD (Earnest Money Deposit) exemption as per GeM General Terms and Conditions (GeM 4.0, Version 1.25, dated 14th July 2025, Page 19) are required to submit a Bid Security Declaration in lieu of EMD. Please refer to RFP, Annexure 4: Bid Security Declaration for the prescribed format. This declaration must be duly filled, signed, and submitted along with the bid documents by vendors seeking the waiver of EMD submission. Failure to submit the Bid Security Declaration (where applicable) will result in the bid being treated as non-responsive.
Bid validity	180 days from the date of opening of the bid.
Performance Bank Guarantee	5% of Project Cost The selected bidder shall be responsible for providing the PBG for the duration of the contract (Including the extension) + claim period (12 months) of the Bank guarantees.
Date of Publishing the tender on Bank's Website	01/10/2026
Last Date for submission of Pre-Bid Query	08/10/2026 Pre bid queries should be submitted as per Annexure 21 in MS Excel format.

	Queries must be mailed to dpo.tp@psb.bank.in only quoting tender reference number in the subject. Subject of the email should be given as "Pre-Bid Queries for PSB/ HO DPO /2026-27/RFP/ RG1 Dated 01/10/2026". Queries reaching afterwards will not be entertained.	
Date and Time for Pre-Bid Meeting	12/10/2026 at 3:00 PM IST Pre-Bid meeting will be held Online, and participants are requested to attend the meeting Online. Those interested in participating the Pre bid meeting should share the participant details to dpo.tp@psb.bank.in Upon perusal of the same, the link / meeting id will be shared with the participant to participate in the virtual meeting.	
Last Date and Time for submission of Bids	22/10/2026 at 3:00 PM IST	
Date and Time of Opening of Bids	22/10/2026 at 3:30 PM IST	
Date and time of opening of online Commercial Bids	To be notified later to the qualifying bidders only.	
Place of Opening of Bids	Punjab & Sind Bank, H.O. Data Protection Office, 2nd Floor, NBCC Building Block 3, East Kidwai Nagar, New Delhi - 110023	
Submission of bids	https://gem.gov.in/	
Contact Persons for any clarifications/ Submission of Bids	Name	Sanjay Kumar
	Designation	Sr. Manager
	Contact No	7011939724
	Name	Naveen Kumar Saini
	Designation	Deputy General Manager
	Email ID	dpo.tp@psb.bank.in
Project Office Location	Punjab & Sind Bank, H.O. Data Protection Office, 2nd Floor, NBCC Building Block 3, East Kidwai Nagar, New Delhi - 110023	
Other Details	Subsequent changes made based on the suggestions and clarifications as per pre-bid meeting shall be deemed	

	to be part of the RFP document and shall be shared with all the bidders. No suggestions or queries shall be entertained after pre-bid meeting. This document can be downloaded from following website: https://punjabandsind.bank.in/, https://gem.gov.in/, and https://eprocure.gov.in/. Any Amendments, modifications, pre-bid replies, clarifications or other communications etc. will be uploaded on the following websites: https://punjabandsind.bank.in, https://gem.gov.in/, and https://eprocure.gov.in/. No individual communication will be sent to the bidders An announcement regarding the publication of the RFP will also be made in newspapers, informing bidders that the document can be downloaded from the following websites: https://punjabandsind.bank.in/, https://gem.gov.in/, and https://eprocure.gov.in/.
Information for Online Participation: The following activities will be conducted online through the https://gem.gov.in/ website: 1. RFP document including all Annexures. 2. Addendums/Corrigendum's to the RFP. 3. Submission of Technical Bid & Commercial Bid by the Bidder. 4. Opening of Technical Bid & Commercial Bid by the Bank. 5. Announcement of results, if any. Instructions: Bidders who wish to participate will have to register with GeM Portal and follow respective guidelines. In case of GeM- related issues contact helpdesk-gem@gov.in In case of any clarification/ queries regarding online registration/ participation, Bidders may reach out to: Email: dpo.tp@psb.bank.in	

* All MSEs(Micro & Small Enterprises) having registration as per provisions of the Public Procurement Policy for Micro and Small Enterprises i.e. District Industries Centre (DIC) or Khadi and Village Industries Commission (KVIC) or Khadi and Industries Board (KVIB) or Coir Board or National Small Industries Commission (NSIC) or directorate of Handicrafts and Handlooms or Udyog Aadhaar Memorandum or any other body specified by Ministry of MSME and Start-ups (recognized by DPIIT) are exempted from

submission of EMD amount only. Relevant Certificates should be submitted by the bidder in this regard to avail exemption

Note:

1. If any of the dates given above happens to be Holiday in Banks in Delhi/NCR, the related activity shall be undertaken on the next working day at the same time.
2. All Claims made by the Bidder will have to be backed by documentary evidence.
3. Bidders should submit bids well before time rather than wait for the last moment to avoid any technical glitches or networking issues etc. at their end.
4. Bidders are requested to use a reliable internet connection (data cable / broadband) to safeguard themselves. The Bank is not responsible for telephone line glitch, internet response issues, hardware hangs etc. at bidder's end.
5. No Claim of any bidder shall be entertained, whatsoever for delayed submission of their bid at any stage because of any reason. Therefore, bidders are advised to submit their bids well before the scheduled time.

2 GLOSSARY

Sr No	Abbreviations	Description / Full form
1.	AMC	Annual Maintenance Contract
2.	API	Application Programming Interface
3.	ARC	Annual Recurring Charges
4.	ATS	Annual Technical Support
5.	Bank / PSB	Punjab & Sind Bank
6.	BCP	Business Continuity Planning
7.	BFSI	Banking, Financial Services, and Insurance
8.	BG	Bank Guarantee
9.	BNS	Bharatiya Nyaya Sanhita
10.	BBPS	Bharat Bill Payment System
11.	BoM	Bill of Material
12.	CBS	Core Banking Solution (Finacle or equivalent).
13.	CBOM	Cryptographic Bill of Materials
14.	CMP	Consent Management Platform.
15.	CSITE	Cyber Security and Information Technology Examination
16.	DC	Data Centre
17.	DG	Data Governance
18.	DPB / DPBI	Data Protection Board of India constituted under the DPDP Act.
19.	DPDP Act	The Digital Personal Data Protection Act, 2023 as amended, modified, re-enacted or brought into force from time to time.

Sr No	Abbreviations	Description / Full form
20.	DPDP Rules	The Digital Personal Data Protection Rules, 2025 notified under the DPDP Act as amended or replaced from time to time, and to the extent in force.
21.	DPIA	Data Protection Impact Assessment.
22.	DPO	Data Protection Officer
23.	DPRM	Data Principal Rights Management.
24.	DR	Disaster Recovery
25.	DWH	Data Warehouse
26.	EMD	Earnest Money Deposit.
27.	EoL	End of Life
28.	EOSL	End of Support life
29.	GCC	General Conditions of Contract
30.	GST	Goods and Service Tax
31.	HO	Head Office
32.	HSM / KMS	Hardware Security Module / Key Management System.
33.	ISO	International Organization for Standards
34.	ITB	Instructions to Bidders
35.	LD	Liquidated Damages
36.	LoA	Letter of Award
37.	LOI	Letter of Intent
38.	MAF	Manufacturer's Authorization Form.
39.	MDM	Master Data Management.
40.	MSE	Micro and Small Enterprises
41.	MSME	Micro, Small and Medium Enterprises
42.	NDA	Non-Disclosure Agreement
43.	NEFT	National Electronic Funds Transfer
44.	NI Act	Negotiable Instruments Act
45.	NIT	Notice Inviting Tender
46.	OEM	Original Equipment Manufacturer
47.	P2P	Point-to-Point
48.	PBG	Performance Bank Guarantee.
49.	PC	Prevention of Corruption Act
50.	PET	Privacy Enhancing Technologies
51.	PO	Purchase Order
52.	PSU	Public Sector Undertaking
53.	QCBS	Quality and Cost-Based Selection.
54.	QoS	Quality of Service
55.	RACI	Responsible, Accountable, Consulted, Informed
56.	RCA	Root Cause Analysis
57.	RFP	Request for Proposal.

Sr No	Abbreviations	Description / Full form
58.	ROPA	Record(s) of Processing Activities.
59.	RTGS	Real Time Gross Settlement
60.	RTO / RPO	Recovery Time Objective / Recovery Point Objective.
61.	SBOM	Software Bill of Materials
62.	SDLC	Software Development Life Cycle
63.	SI	System Integrator
64.	SIEM / SOC	Security Information and Event Management / Security Operations Centre.
65.	SLA	Service Level Agreement
66.	TCO	Total Cost of Ownership
67.	TIS	Tender Information Summary
68.	ToS	Type of Service
69.	UAT	User Acceptance Testing
70.	VAPT	Vulnerability Assessment and Penetration Testing.

3 DISCLAIMER

- The information contained in this Request for Proposal (RFP document) or any information provided subsequently to Bidder(s) in documentary form by or on behalf of the Bank, is provided to the Bidder(s) on the terms and conditions set out in this RFP document and all other terms and conditions subject to which such information is provided. This document shall not be transferred, reproduced or otherwise used for purposes other than for which it is specifically issued.
- This RFP is neither an agreement nor an offer and is only an invitation by the Bank to the interested parties for submission of bids. No contractual obligation whatsoever shall arise from the RFP process until a formal contract is executed by the duly authorized signatory of the Bank and the Bidder. The purpose of this RFP is to provide the Bidder(s) with information to assist in the formulation of their proposals.
- This RFP does not claim to contain all the information each bidder may require. Each Bidder should conduct its own investigations and analysis and is free to check the accuracy, reliability, and completeness of the information in this RFP and obtain independent advice, wherever necessary. Bank may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP.
- The Bank reserves the right to reject any or all Request for Proposals received in response to this RFP document at any stage without assigning any reason whatsoever. The decision of Punjab & Sind Bank shall be final, conclusive, and binding on all the parties.
- This RFP Document may not be appropriate for all people, and it is not possible for the Bank Representatives, their employees, or advisors to consider the investment objectives, financial situation and particular needs of each party who reads or uses this RFP Document.

- The Bank, its employees and advisors make no representation or warranty and shall have no liability to any person, including any Applicant or Bidder under any law, statute, rules or regulations or tort, principles of restitution or unjust enrichment or otherwise for any loss, damages, cost or expense which may arise from or be incurred or suffered on account of anything contained in this RFP or otherwise, including the accuracy, adequacy, correctness, completeness or reliability of the RFP and any assessment, assumption, statement or information contained therein or deemed to form or arising in any way for participation in this bidding process.
- The Bank also accepts no liability of any nature whether resulting from negligence or otherwise, howsoever caused arising from reliance of any Bidder upon the statements contained in this RFP.
- The issue of this RFP does not imply that the Bank is bound to select a Bidder or to appoint the selected Bidder, for the Project and the Bank reserves the right to reject all or any of the Bids without assigning any reason whatsoever.
- No Bidder or its associate shall submit more than one Bid for the Scope of Work as desired under this RFP. A Bidder applying individually or as an associate shall not be entitled to submit another Bid either individually or through associates, as the case may be.
- This RFP, the bidding process and any Contract resulting from it shall be governed by the laws of India. Courts at New Delhi shall have exclusive jurisdiction, subject to the dispute resolution provisions of the Contract.

4 INTRODUCTION

Punjab & Sind Bank, (hereinafter referred to as “Bank” a body corporate constituted under the Banking Companies (Acquisition and Transfer of Undertakings) Act, 1980, one of the nationalized Banks of India, has a national presence through a widespread network of 1692+ branches, 5 Zonal Offices and 34 Regional Offices all networked under Centralized Banking Solution. It also has a network of 1188+ ATMs spread across the country including onsite and offsite ATMs. With more than 119 years of customer services, the Bank has a large, satisfied clientele throughout the country. For enhancing customer convenience levels and overall inter-branch efficiency, the Bank has been a frontrunner in implementing various IT enabled products.

For Implementing DPDP compliance in the Bank, the Bank invites a Request for Proposal for **Procurement of DPDP Suite and selection of System Integrator (SI) cum Consultant services for Supply, Installation, Integration, Implementation and Management of Digital Personal Data Protection Solution for a period of 3 Years**

5 PROJECT OBJECTIVE

To procure, deploy, implement, integrate, support and manage a robust, Digital Personal Data Protection Suite and consultancy services to ensure comprehensive compliance with the Digital Personal Data Protection (DPDP) Act/ Rules. The solution

must automate the lifecycle of collecting, managing, verifying, and enforcing user consent, Data Discovery and Classification, Data Principal Rights, ROPA, DPIA, Grievance Redressal, notifications to data principal and report to DPBI and other reporting and audit for personal data processing across the Bank's enterprise level.

The Bank invites bids as per the specifications indicated in **scope of work** mentioned in the RFP document. The prices quoted by the selected bidder remain valid for all orders placed with the selected bidder for the entire contract period and duly accepted by the bidder. The interested bidders are requested to send their technical proposal and Commercial proposal as per the enclosed formats. (Appendix 2)

5.1 Purpose

1. The Primary Goal is compliance and absolute alignment with the Digital Personal Data Protection (DPDP) Act and DPDP Rules.
2. The selected bidder/vendor shall assume end-to-end responsibility for **Procuring**, provisioning, configuring, implementing and maintaining the Digital Personal Data Protection Suite, in scope solutions and infrastructure.
3. Achieve end-to-end, verifiable, auditable compliance with the DPDP Act and DPDP Rules across the Bank's applications including third-party/processor, upstream-downstream and all other processes at enterprise level.
4. Design and implement an integrated DPDP Suite covering and associated activities
 - a) Notice & Consent Management
 - b) Cookie Management
 - c) Data Principal Rights Management
 - d) Third Party Risk Management
 - e) Personal Data Discovery and Data Security Posture Management
 - f) Records of Processing Activities / Data Protection Impact Assessment
 - g) Data Breach and Incident Management
 - h) Privacy Enhancing Technologies
 - i) Privacy Threat Modelling
 - j) Privacy Training Awareness
 - k) Dashboards and Reporting , Audit Logs

Note: Immutable and auditable Records of activities/logs to be maintained as per DPDP Act, the Bank's record-retention schedule and regulatory directions. Where different periods apply, the longer period shall prevail, unless deletion is mandatorily required by law.

5. The Bidder shall ensure that the proposed solution architecture supports full DC-DR replication and failover for all in-scope modules, with Recovery Time Objective (RTO) and Recovery Point Objective (RPO) as per specs defined in RFP and not exceeding industry-standard thresholds for BFSI production systems and shall conduct DR drills as and when required.
6. The Project comprises following streams delivered by Bidder:

- i. Consulting Services – Covering the advisory, operational, legal and regulatory compliance etc.
 - ii. System Integration Services - Procurement, configuration, integration, testing, go-live, operation & maintenance of the DPDP Suite and other solutions including associated hardware/ infrastructure, software licenses, and on-site resource deployment as detailed in RFP document for the period of 3 Years.
7. Implement Board-approved policies, SOPs, a RACI-based governance operating model, and a trained, change-ready organization.
 8. Provide 3 years of stable, SLA-governed operations, support and continuous compliance monitoring, with DPBI-ready evidence and reporting.

6 INSTRUCTIONS TO BIDDERS

6.1 Language of the Bid

The bid as well as all correspondence and documents relating to the bid exchanged by the Bidder and the Bank shall be in English language only.

6.2 Bid Currency & Price Structure

Prices shall be expressed in the Indian Rupees (INR) only, the bidder must quote price exclusive of all applicable GST. **The cost will not depend on any variation in the dollar or any exchange rate/change in tax structure.**

6.3 Bid System Offer

1. The Bid Proposal being submitted would be binding on the Bidder. As such it is mandatory that authorized personnel of the firm or organization sign the Bid. The designated personnel should be authorized by a senior official of the Organization having such authority to do so. The same person or a different person should be authorized who should have authority to quote. The Xerox copy of necessary Original Resolutions/ Authority/ Power of Attorney having authority to authorize the person to submit Bid Documents, on behalf of the Company shall be enclosed. The proposal must be accompanied by an undertaking letter duly signed by the designated personnel providing a Bid commitment. The letter should also indicate the complete name and designation of the designated personnel.
2. The bidder shall submit his response to the present tender with the price which will contain the pricing information.
3. Any effort by a Bidder to influence the Bank in evaluation of his bid, bid comparison or contract award decision would result in the rejection of the said bid. The Bank's decision in this case would be final and without prejudice and will be binding on all parties.
4. The Bank reserves the right to accept or not to accept any bid or to reject a particular bid at its sole discretion without assigning any reason whatsoever.

5. The Bids containing erasures or alterations will not be considered. There should be no handwritten material, corrections or alterations in the Bids. All details must be filled in.
6. Bidder staff, personnel and labour will be liable to pay personal income taxes in India in respect of such of their salaries and wages as are chargeable under the laws and regulations for the time being in force, and Bidder shall perform such duties regarding such deductions thereof as may be imposed on him by such laws and regulations.
7. Bidder warrants that it shall be solely liable and responsible for compliance of applicable Labour Laws in respect of its employee, agents, representatives and subcontractors (if allowed) and in particular laws relating to terminal benefits such as pension, gratuity, provident fund, bonus or other benefits to which they may be entitled and the laws relating to contract labour, minimum wages, etc., and the Bank shall have no liability in this regard.

6.4 Two Bid System:

This is two-bid system which has the following 2 parts:

Part A- Technical cum Eligibility Proposal: Indicating the response to the Pre-Qualification Criteria, Technical evaluation criteria, Appendix & annexures for Technical and Eligibility requirement, Compliance to Scope of Work and other terms & conditions. The format for submission of Technical Proposal is as per:

Annexure 1: Submission checklist along with Appendix 1: Functional & Technical Compliance Sheet, Appendix 2: - Masked Commercial Bill of Material.

Part B-Commercial Bid: Furnishing all relevant information as required as per Bill of Material as per Appendix 2. The format for submission of Commercial bid is as per Annexure 13.

6.4.1 Preparation of Bids:

6.4.1.1 Part A – Technical cum Eligibility Proposal

1. Before submitting the bid, the bidders should ensure that they conform to the Pre-Qualification Criteria as stated in RFP. Only after satisfying themselves of the Pre-Qualification Criteria, the Offer should be submitted as per 10.2 Eligibility Qualification Criteria
2. Technical cum eligibility Proposal should be submitted as per the format in Annexure 1: Submission Checklist. Relevant technical details and documentation should be provided along with Technical Proposal.
3. It is mandatory to provide compliance with the scope required by the Bank.
4. The offer may not be evaluated and may be rejected by the Bank without any further reference in case of non-adherence to the format or partial submission of technical information as per the format given in the offer.

5. The Bank shall not allow / permit changes in the technical/functional requirements once it is submitted.
6. The relevant solution information, brand, and solution offered, printed product brochure, technical/functional specification sheets etc. should be submitted along with the Offer. Failure to submit this information along with the offer may result in disqualification.
7. The Technical Proposal should be complete in all respects and contain all the information sought for. **Masked Bill of Material/ Commercial Bid** must be attached in Technical Offer and should not contain any price information. The Part A - Technical cum Eligibility Proposal should be complete and should cover all products and services. **Technical Proposal without masked Commercial Bid/Bill of Materials will be liable for rejection.** Masked Bill of Material which is not as per instruction will make Bid liable for rejection. Masked bill of material should be a replica of actual Bill of Material except that it should not contain any price information (with Prices masked). It should not provide any price information like unit price, tax percentage, tax amount etc.

6.4.1.2 Part B - Commercial Bid

1. Commercial Bid should be submitted as per instruction in **Annexure 13**.
2. Commercial Bid shall be submitted as per Bill of Material and other terms and conditions of RFP on prices. The Commercial Bid should give all relevant price information as per **Annexure 13**. Any deviations from the Bill of Material / non submission of prices as per the format shall make the bid liable for rejection.
3. The bidder must quote the best competitive price in the commercial bid.
4. The bid must be made in an organized and structured manner.

*Note: All Claims made by the Bidder will have to be backed by documentary evidence. The bidder is expected to examine all instructions, forms, terms and specifications in the RFP. Failure to furnish all the information required or to submit a Bid not substantially responsive to the RFP in every respect will be at the Bidder's risk and may result in the rejection of the Bid. No request for any change to the commercial or legal terms and conditions of this RFP, except as provided in the RFP or in any addendum, corrigendum or clarification issued by the Bank, shall be entertained. Queries / requests seeking any such change shall not be entertained.

6.5 Cost of Preparation

The Bidder shall bear all costs associated with the preparation and submission of its Bid and the Bank will in no case be responsible or liable for these costs, regardless of the conduct or outcome of the Bidding process.

6.6 Normalization of Bids

The Bank will go through a process of technical evaluation and normalization of the bids to the extent possible and feasible to ensure that Bidders are on the same technical

ground. After the normalization process, if the Bank feels that any of the bids needs to be normalized and that such normalization has a bearing on the commercial bid; the Bank may at its discretion ask all the technically shortlisted Bidders to resubmit the technical and commercial bids once again for scrutiny. The Bank can repeat this normalization process at every stage of technical submission or till the Bank is satisfied. The Bidders agree that they have no reservation or objection to the normalization process and all the technically short-listed Bidders will, by responding to this RFP, agree to participate in the normalization process and extend their co-operation to the Bank during this process. The Bidders, by submitting the response to this RFP, agree to the process and conditions of the normalization process.

6.7 Submission of Bid and communication

The Bank expects the bidders to carefully examine all instructions, terms and conditions mentioned in this RFP document before submitting its unconditional compliance as part of the RFP. The bidders shall independently review and assess the information contained in this RFP and any addenda, corrigenda or clarifications issued in connection with it, and form their own opinions and conclusions regarding the matters contained therein. The issue of this RFP or any such addenda, corrigenda or clarifications does not relieve the bidders of their responsibility to make their own assessment before submitting their Bids. Failure to furnish all information required or submission not substantially responsive to the RFP in every respect will be at the bidder's risk and may result in the rejection of Bids.

Bids duly signed and sealed is to be submitted in following form on or before the last Date and Time for bid submission as defined in the Section 1: Key information:

1. The Technical Bid shall be submitted online through the GeM Portal
2. Commercial Bid – Only Online (on GEM Portal)

Any other mode of submission, e.g. by fax, e-mail etc. will not be accepted. No Claim of any Bidder(s) shall be entertained, whatsoever for delayed submission of their bid at any stage because of any reason. Therefore, Bidder (s) are advised to submit their bid well before the scheduled time.

Bids will be opened in the presence of the bidder representatives who choose to attend the opening of tender on the specified date, time and place of bid opening. No separate intimation will be given in this regard.

Bank reserves its right, at its sole discretion to cancel or withdraw the order even after issuing the letter of Intent (LOI) / Purchase Order, if bank receives any directions / orders/ instruction or communication from Statutory Body / RBI/Govt. of India or any other competent authority requiring or directing the bank not to take the project forward or any reasons whatsoever. The decision of the Bank shall be final in this regard without disclosing any reason to any bidder or person.

6.8 Late bids

1. Any bid received after the due date and time for receipts of bids as prescribed in this RFP will be rejected. However, in case of the specified date of submission of bids being declared a holiday for the Bank, the bids will be received up to the specified time on the next working day.
2. The Bank may, at its discretion, extend this deadline for submission of bids by amending the bid documents, in which case all rights and obligations of the Bank and bidders, previously subject to the deadline, will thereafter be subject to the deadline extended.
3. All such information will be published on Bank's website or <https://gem.gov.in/> only. The bidders have to take note of it.
4. The Bidder must submit the bids as specified above in section 6.7. Failure to submit the bid in the specified process shall render the bid ineligible for evaluation.

6.9 Modifications and/ or Withdrawal of Bids

1. Bids once submitted will be treated as final and no modification will be permitted. No Correspondence in this regard will be entertained.
2. The Bid should contain no alterations, erasures, or overwriting. The Bidder is expected to examine all instructions, forms, terms and specifications in the bidding documents. Failure to furnish all information required by the bidding documents or submission of bid not substantially / conclusively responsive to the bidding documents in every respect will be at the Bidders risk and may result in rejection of the bid.
3. No bidder shall be allowed to withdraw the bid after the deadline for submission of bids.
4. In the case of the successful bidder, he will not be allowed to withdraw/back from the bid commitments. The bid earnest money in such eventuality shall be forfeited, and all interests/claims of such bidder shall be deemed as foreclosed

6.10 Earnest Money Deposit (EMD)

1. The bidder shall furnish Non-interest Earning Earnest Money Deposit (EMD) amount (Rs 70 lakh) as mentioned in the Bid Schedule by way of Bank Guarantee drawn on any Scheduled Bank in India (except Cooperative Bank, RRB & Punjab & Sind Bank) in favor of Punjab & Sind Bank, payable at Delhi.
2. The same should be valid for an additional 45 days beyond bid validity period. Bank at its discretion can demand for extension for the validity of EMD. The format for submission of EMD in the form of Bank Guarantee is as per **Annexure 14**.
3. The Bank Guarantee issued by the issuing Bank on behalf of Bidder in favor of Bank shall be in paper form as well as issued under the "Structured Financial Messaging System" (SFMS) sent to Punjab & Sind Bank, Sector 44 Branch, Gurgaon, IFSC PSIB0021509. Any **Bank guarantee submitted in physical mode**, including EMD/bid guarantee which cannot be verifiable through SFMS will be rejected summarily.

4. Non submission of EMD will lead to rejection of Bid.
5. All MSEs having registration as per provisions of the Public Procurement Policy for Micro and Small Enterprises i.e. District Industries Centre (DIC) or Khadi and Village Industries Commission (KVIC) or Khadi and Industries Board (KVIB) or Coir Board or National Small Industries Commission (NSIC) or directorate of Handicrafts and Handlooms or Udyog Aadhaar Memorandum or any other body specified by Ministry of MSME and Start-ups (recognized by DPIIT) are exempted from submission of EMD only. Relevant certificates should be submitted by the bidder in this regard to avail of exemption. Bid Security Declaration should be submitted by eligible MSEs/Startups on Company's letter head with company seal and signature of the authorized person as per **Annexure-4**.
6. The EMD may be forfeited/ Bank Guarantee may be invoked:
 - a) If the bidder withdraws/amends the bid during the period of bid validity (180 days from the date of opening of bid).
 - b) If the bidder makes any statement or encloses any form which turns out to be false, incorrect and / or misleading at any time prior to signing of contract and/or conceals or suppresses material information; and / or
 - c) The selected bidder withdraws his tender before furnishing the unconditional and irrevocable Performance Bank Guarantee.
 - d) The bidder violates any of the provisions of the terms and conditions of this tender specification.
 - e) In case of the successful bidder, if the bidder fails:
 - i. To sign the contract in the form and manner to the satisfaction of Punjab & Sind Bank.
 - ii. To furnish the Performance Bank Guarantee in the form and manner to the satisfaction of Punjab & Sind Bank.
 - iii. Bank may proceed against the selected bidder in the event of any evasion, avoidance, refusal or delay on the part of the bidder to sign and execute the Purchase Order / Service Level Agreements or any other documents, as may be required by the Bank, if the bid is accepted.
 - iv. The Execution of Bid Security Declaration/ Invocation of EMD may suspend participation of the Bidder in any tender in this Bank for three (03) years.
7. Bid securities of the unsuccessful bidders will be returned to them at the earliest after expiry of the final bid validity and latest on or before the 30th day after the award of the contract. The EMD of the selected bidder will be returned within 15 days after submission of Performance Security (PBG) and execution of Contract with the Bank.

6.11 Performance Bank Guarantee/Security Deposit (PBG)

1. The amount of PBG is 5% of total contract value
2. The successful bidder/s should submit a Security Deposit / Performance Guarantee as specified in **Key Information within 30 days from the date of acceptance of Purchase Order**.

3. Security Deposit / Performance Guarantee should be submitted by way of Bank Guarantee in favor of Punjab & Sind Bank payable at Delhi / Bank Guarantee may be obtained from any of the Scheduled Commercial Banks (except Cooperative Bank, RRB & Punjab & Sind Bank) for an amount as mentioned in Section 1: **KEY INFORMATION.**
4. The selected bidder shall be responsible for providing the PBG for the duration and validity of entire **original Contract Period (i.e., Implementation Period + 36 months of Support Services), along with a claim period of 12 months.** In case the Bank exercises its option to extend the Contract beyond the original Contract Period, for up to **two (2) additional years** in one-year increments, the Selected Bidder shall be required to extend the validity of the PBG corresponding to the extended Contract Period, along with the additional 12-month claim period.
5. The Bank Guarantee issued by the issuing Bank on behalf of Bidder in favor of Punjab & Sind Bank shall be in paper form as well as issued under the "Structured Financial Messaging System" (SFMS) sent to Punjab & Sind Bank, Sector 44 Branch, Gurgaon, IFSC PSIB0021509. Any Bank guarantee submitted in physical mode, including EMD/bid guarantee which cannot be verifiable through SFMS will be summarily rejected.
6. The PBG applicable must be duly accompanied by a forwarding letter issued by the issuing Bank on the printed letterhead of the issuing Bank.
7. Security Deposit/Performance Bank Guarantee should be valid for the complete duration of contract period (Including the extension) + claim period (12 months).
8. The selected bidder shall be responsible for extending the validity date and claim period of the Bank guarantees as and when it is due, on account of non-completion of the project and contract period.
9. In the event of the Service Provider committing a breach of the terms and conditions of the contract, Bank shall provide a cure period of 30 days and thereafter invoke the PBG if the Service Provider is unable to service the contract for whatever reason.

6.12 No commitment to accept lowest or any bid

The Bank shall be under no obligation to accept the lowest or any other offer received in response to this tender notice and shall be entitled to reject any or all offers including those received late or incomplete.

The Bank reserves the right to make changes in terms and conditions of purchase. Bank will be under no obligation to have discussions with any bidder, and/or entertain any representation.

After Contract award, any change to scope, architecture, hosting location, sub-processors, material security controls, deliverables, timelines or charges shall be effective only through a written change-control document approved by the Bank's authorised signatory. Operational discussions, meeting minutes, emails from project personnel, silence or use of a deliverable shall not amend the Contract or authorise additional charges.

6.13 Right to Accept Any Bid and to Reject Any OR All Bids/Cancellation of Tender process

Punjab & Sind Bank reserves the right to accept or reject in part or full any or all offers without assigning any reason thereof even after issuance of letter of Intent. Any decision of Punjab & Sind Bank in this regard shall be final, conclusive and binding upon the bidders. The Bank reserves the right to accept or reject any Bid in part or in full, and to annul the Bidding process and reject all Bids at any time prior to contract award, without thereby incurring any liability to the affected Bidder or Bidders or any obligation to inform the affected Bidder or Bidders of the grounds for Bank's action. During any stage of evaluation process, if it is found that the bidder does not meet the eligibility criteria or has submitted false /incorrect information the bid will be summarily rejected by the Bank and no further correspondence would be entertained in this regard. The Bank reserves the right to amend, rescind, reissue or cancel this RFP and all amendments will be advised to the Bidder, and such amendments will be binding upon them. The Bank also reserves its right to accept, reject or cancel any or all responses to this RFP without assigning any reason whatsoever. Further please note that the Bank would be under no obligation to acquire any or all the items proposed. No contractual obligation whatsoever shall arise from the RFP process unless and until a formal contract is signed and executed by duly authorized officials of Punjab & Sind Bank and the bidder.

6.14 Correction of Errors

Bidders are advised to exercise greatest care in entering the pricing figures. No corrigendum or requests for prices to be corrected will be entertained after the bids are opened. If there are any corrections in the bid document, the authorized signatory should initial them all, failing which the figures for such item shall not be considered. Discrepancies in bids will be corrected as follows:

1. Where there is a discrepancy between the amounts in figures and in words, the amount in words shall prevail.
2. If there is a discrepancy between percentage and amount, the amount calculated as per the stipulated percentage basis shall prevail
3. Where there is a discrepancy between the unit rate and the line-item total resulting from multiplying the unit rate by the quantity, the unit rate will govern unless, in the opinion of Bank, there is an obvious error such as a misplacement of a decimal point, in which case the line-item total will prevail.
4. Where there is a discrepancy between the amount mentioned in the bid and the line-item total present in the schedule of prices, the amount obtained on totaling the line items in the Bill of Materials will prevail.
5. The amount stated in the correction form, adjusted in accordance with the above procedure, shall be considered as binding, unless it causes the overall price to rise, in which case the bid price shall prevail.
6. In case the bidder does not accept the correction of the errors as stated above, the bid shall be rejected.

7. The Highest Technical bidder shall not automatically qualify for becoming a selected bidder and for award of contract by the Bank.
8. The Lowest Commercial Bidder shall not automatically qualify for becoming selected Bidder and for award of contract by the Bank.
9. The commercials will be calculated till two decimal points only. If the third decimal point is greater than .005 the same shall be scaled up else, it shall be scaled down to arrive at two decimal points. Bank will make similar treatment for 4th or subsequent decimal point to finally arrive at two decimal points only.
10. If for some reason, negotiations with the successful bidder fail to result in an agreement within a specified timeline, the Bank reserves the right to award the contract to the next most eligible bidder based on the evaluation.
11. The Bank shall not incur any liability to the affected Bidder on account of such rejection.

Based on the Bank's requirements as listed in this document, the bidder should identify and offer the best-suited solution / bill of material for the product that would meet the Bank's requirements and quote for the same.

During the Tendering process, if any event of conflict arises between the content of the Annexures submitted by bidders and the main body of RFP, then the content of main RFP shall prevail/ applicable.

6.15 Soft copy of tender document

The soft copy of the tender document will be made available on the Bank's website <https://gem.gov.in/> , <https://eprocure.gov.in/> & <https://punjabandsind.bank.in> . However, the Bank shall not be held responsible in any way, for any errors / omissions /mistakes in the downloaded copy.

6.16 Bid validity period

Bids shall remain valid for the period as defined in section 1: Key Information. The Bank holds the right to reject a bid valid for a period shorter than validity period defined in the RFP as non-responsive, without any correspondence. In exceptional circumstances, The Bank may solicit the Bidder's consent to an extension of the validity period. The request and the response thereto shall be made in writing. The extension of validity period by the Bidder should be unconditional and irrevocable. The Bid Security provided should also be suitably extended.

A Bidder acceding to the request will neither be required nor be permitted to modify its bid. A Bidder may refuse the request without forfeiting its bid security. In any case the bid security of the Bidders will be returned after completion of the process.

6.17 Pre-bid meeting

For clarification of doubts of the bidders on issues related to this RFP, the Bank intends to hold a Pre-Bid Meeting on the date and time as indicated in the RFP in Key-Information.

For any clarification with respect to this RFP, the bidder may send an email to dpo.tp@psb.bank.in by last date of submission of queries as defined in Key-Information in this document. Any queries or requests for clarification received after the stipulated time shall not be entertained.

If the meeting date is declared as a holiday under NI Act by the Government after issuance of RFP, the next working day will be deemed to be the pre-bid meeting day.

The format to be used for seeking clarification is mentioned in **Annexure 21** (Pre-bid Query Format). It may be noted that all queries, clarifications, questions etc., relating to this RFP, technical or otherwise, must be in writing only and should be sent to the email-id as stated earlier. No oral or individual consultation will be entertained.

The Bank does not have the responsibility to consider any other queries raised by the bidder's representative during the pre-bid meeting.

Participation in the Pre-Bid Meeting shall be restricted to duly authorized representatives of the bidder. The bidder shall submit an authorization letter, duly signed by its authorized signatory, for each representative attending the meeting.

Additionally, the bidder shall share the names, designations, organization details, mobile numbers, and email addresses of the attendees with the Bank at least one (1) working day prior to the date of the Pre-Bid Meeting.

The Bank reserves the right to deny participation to representatives whose details have not been communicated within the stipulated timeline.

The Bank will consolidate all the queries and any further queries during the pre-bid meeting and the replies for the queries shall be made available to all the bidders. The clarification of the Bank in response to the queries raised by the bidder/s, and any other clarification/amendments/corrigendum furnished thereof will become part and parcel of the RFP and it will be binding on the bidders.

The Bank reserves the right not to entertain or respond to any query, clarification request, or representation received after the prescribed deadline for submission of pre-bid queries.

Non-response by the Bank to any query, clarification, or issue raised by a bidder during the Pre Bid Meeting shall not be deemed acceptance or concurrence by the Bank. Only responses and clarifications formally communicated by the Bank in writing shall be treated as valid and binding.

6.18 Amendment to RFP Contents

At any time prior to the last date for bid-submission, the Bank may, for any reason, whether at its own initiative or in response to clarification(s) requested by a prospective bidder, modify the RFP contents by issuing Corrigendum. However, it is the bidder's responsibility to keep its communication channels (face-to-face, phone, fax, e-mail etc.) alive including observing Bank's website for the latest development in this regard. The Bank will not be liable for any communication gap. To provide prospective bidders,

reasonable time to take the amendment into account for preparation of their bid, the Bank may, at its discretion, extend the last date for bid-submission.

The Bank reserves the right to scrap the tender at any stage without assigning any reason.

6.19 Disqualification

Any form of canvassing/ lobbying/ influence/ query regarding short listing, status etc. will result in disqualification.

6.20 Fixed Price

The prices quoted in the tender response will be fixed for the period of the contract. The price should be exclusive of GST.

6.21 Project Execution

The project shall be executed and completed in a timely and expeditious manner as per the timelines prescribed by the Bank. The Bank and the selected bidder/s shall nominate a Project Manager immediately on acceptance of the order, who shall be the single point of contact for the project. However, for escalation purposes, details of other persons shall also be given. The project manager nominated by the bidder/s should have prior experience in implementing a similar project and meet eligibility criteria as defined in RFP

6.22 Confidentiality of the Bid Document

The Bidder, irrespective of his/her participation in the bidding process, shall treat the details of the documents as secret and confidential.

7 SCOPE OF WORK

This Scope of Work applies to each module/tool proposed under this RFP, whether delivered individually or as an integrated suite. The Bidder shall Procure, implement and manage a comprehensive end-to-end solution as per industry's best practices ensuring full compliance with the DPDP Act, DPDP Rules and other applicable laws that are in force from time to time during the Contract across all modules till the currency of Contract Tenure. Bidder must ensure solution design, configuration and customization is as per Bank's requirement & scalability as defined in the RFP.

7.1 System Integrator (SI) cum Consultant — Scope of Work & Responsibilities

The Bank intends to engage a bidder as **SI-cum-Consultant** for Digital Personal Data Protection Act, 2023 (DPDP) compliance. The selected bidder shall be the **single point of contact** to the Bank for both advisory/compliance and technical delivery.

The Bank shall retain ownership of all policy, risk-acceptance, legal-basis and regulatory decisions. The selected bidder shall act only on documented instructions of

the Bank and shall not represent that any tool configuration, certification or deliverable by itself constitutes legal compliance or transfers the Bank's statutory accountability.

1. The bidder shall carry out, without limitation, the responsibilities set out below and in the wider Scope of the RFP and shall ensure that technical controls implemented remain synchronised with, and demonstrably enforced, best industry practices, the Board-approved DPDP policies and SOPs.
2. All deliverables shall be of a standard suitable for submission to the Bank's Board, Internal Audit, Statutory Auditors, RBI and the Data Protection Board of India (DPB) or any other regulator/ Statutory Authority.

7.1.1 Objectives

1. **Procure, Implement and operationalise** the full DPDP Solution suite i.e. Notice & Consent Management, Cookie Management, Data Principal Rights Management, Third Party Risk Management, Personal Data Discovery and Data Security Posture Management, Records of Processing Activities / Data Protection Impact Assessment, Data Breach and Incident Management, Privacy Enhancing Technologies, Privacy Threat Modelling, Privacy Training Awareness, Dashboard and Reporting across the Bank's application, channels, data touchpoints including application hosted at public/private cloud of Bank at enterprise level.
2. Achieve and sustain enterprise-wide compliance with the DPDP Act, the DPDP Rules, applicable RBI guidelines/Master Directions and CERT-In directions across all applications, functions and digital and physical channels.
3. Embed due care, due diligence and Privacy-by-Design as standing enterprise disciplines rather than one-time activities.
4. Provide sustained consultancy, governance, monitoring, training, audit and regulatory readiness, and a structured knowledge transfer and exit.

7.1.2 Coverage

1. **Organisational units:** Head Office, Corporate Centre, Zonal and Regional Offices, all branches, Central Processing Centres, back-offices, International Banking Unit, administrative offices any other data processing /touchpoint.
2. **Third Party/Vendor:**
 - i. Include all third-party processors, sub-processors and outsourced arrangements handling personal data, mapped to data elements, purpose and hosting location.
 - ii. Covers all vendor contracts/SLAs against Section 8(2) of the DPDP Act and DPDP Rules and provide standard clauses covering security safeguards, breach intimation, sub-processing, audit rights and data deletion on exit.

3. **Functions/Departments/Verticals:** IT, Digital Banking, Information Security (CISO), Legal, Compliance, Risk, HR, Operations, all Business verticals, Marketing, Grievance/Customer Service Cell, Vendor & Procurement Management, Internal Audit, Cloud/Infrastructure, Board Secretariat and any other department identified by the Bank.
4. **Channels:** Branch/physical, Digital Channels (Internet Banking, Mobile Banking etc), IVR/call centre, chatbot/WhatsApp, website, ATM/CRM, payment gateways and partner APIs (Account Aggregator, BBPS, UPI, CBDC etc and similar).
5. **Applications/Processes:** 250 applications, 4500+ Process and systems across on-premises, private/public cloud and SaaS including CBS, CRM, LOS/LMS, HRMS, DWH/Data Lake, DMS, email/SMS gateways and digital banking platforms, all upstream and downstream applications.
6. **Data domains:** Customer, employee, applicant/prospect, vendor/contractor, children's and persons-with-disability data, transaction and behavioural data, biometric/Aadhaar-linked data, call recordings, CCTV footage, cookies and digital-tracking data etc.
7. **Records:** Digital, phygital and physical/manual records, including archived, legacy and third party-held records.
*Counts stated are indicative, and shall be finalised during Gap Assessment, and **do not caps the actual scope** — full scope delivery is the compliance coverage governing principle.

7.1.3 Consultant (Advisory, Legal & Compliance) Responsibilities

1. **Strategy, Architecture & Documentation.** Prepare and maintain the overall DPDP compliance strategy, the implementation approach, and the enterprise architecture before and after CMP deployment. Maintain the complete documentation set in version-controlled, audit-ready form: Business Requirements Document, Change Requirement Documents, HLD/LLD, solution and integration architecture (downstream applications, data points etc.), data-flow diagrams and lineage, and as-built documentation.
2. **Gap Assessment & Remediation Roadmap.** Conduct, or review, an enterprise-level gap assessment. Map each control against the DPDP Act, the DPDP Rules, RBI directions and other statutory guidelines. Produce a risk-rated gap heat-map and a remediation roadmap and refresh the assessment periodically. Gap assessment report to be prepared to submit to Board.
3. **Personal Data Inventory & ROPA.** Validate the Bank's Personal Data Inventory (PII/SPI) and Record of Processing Activities. Coverage includes CBS, CRM, LOS/LMS, mobile and internet banking, payments, HRMS, DWH, vendor systems, all channels and physical records. For each processing activity, map the purpose, legal basis, data flow, retention and cross-border transfer.

4. **Privacy Policy & Governing SOPs.** Draft, review and periodically update the enterprise Data Protection & Privacy Policy. Prepare SOPs/frameworks not covered under the specific modules below:
 - i. Data Retention, Archival & Erasure
 - ii. Data Security Posture Management
 - iii. Personal data of Persons with Disabilities and children, including verifiable parental/guardian consent
 - iv. Audits, Notifications & Reports
 - v. Enterprise Privacy-by-Design Checklist
 - vi. Data Processing Agreements
5. **Data Fiduciary & Significant Data Fiduciary Obligations.** Conduct a Significant Data Fiduciary (SDF) applicability assessment. Advise the Bank on its obligations as a Data Fiduciary and any additional SDF obligations, including DPIA periodicity, engagement of an independent data auditor, and algorithmic due diligence.
6. **DPO Function & Privacy Governance.** Design and support operationalization of the DPO function, the internal privacy governance structure, the Privacy Office operating model, and reporting lines to the Board or Board Committee.
7. **Privacy Notices & Consent Artefacts.** Draft and update privacy notices and consent artefacts for customers and employees, across digital and physical channels.
 - i. Languages: English, Hindi and the Eighth Schedule languages as applicable.
 - ii. Scope: layered notices, cookie notices, and revised account-opening, KYC, loan and HR forms, in line with the DPDP Act and Rules.
8. **Consent Management Framework & SOP.** Design the enterprise consent framework, covering:
 - i. consent capture and purpose-wise granularity
 - ii. withdrawal of consent
 - iii. the deemed consent / legitimate-uses register and its governance
 - iv. consent versioning, and reconfirmation when a policy or purpose changes
 - v. a re-consent strategy for the existing customer base
 - vi. migration of legacy and manual consent records
9. **Data Principal Rights & Grievance Redressal Framework & SOP.** Design the framework for access, correction, completion, updation, erasure, nomination, consent withdrawal and grievance redressal. Cover both digital self-service and branch/non-digital intake, with identity verification, SLAs and an escalation matrix.
10. **Breach Response & Notification Framework & SOP.** Design the breach response and notification framework aligned to DPDP, CERT-In and RBI

reporting obligations. Update the Bank's Incident Response Plan and BCP accordingly.

11. DPIA Framework, Methodology & Execution. Design the DPIA methodology, using a hybrid of automated and expert-led assessment. Conduct DPIAs for high-risk, new and materially changed processing activities, including on-premise and cloud-hosted applications. Maintain the DPIA register and action tracker through to closure.

12. Vendor, Processor & Cloud Service Provider Management. Prepare the framework/SOP for periodic due diligence and conduct due diligence of vendors, processors and Cloud Service Providers. Draft DPDP-aligned contract clauses and data-processing agreements, and support re-papering of existing contracts. Track vendor remediation to closure and support periodic re-certification.

13. Cross-Border Transfer & Data Localisation. Assess cross-border transfer and data localisation arrangements, including cloud hosting locations and RBI data-localisation requirements. Maintain a cross-border transfer register. Assess applicability of other international data regulations (e.g., GDPR) for enterprise-level processes.

14. Regulatory Change Management & Legal Advisory.

Track MeitY notifications, DPDP Rules amendments, DPB orders and precedents, RBI circulars and CERT-In directions throughout the term. Assess the impact of each, and recommend policy, process and contractual changes, with version-controlled updates to all affected documents.

Provide ongoing advisory support to the DPO Office, Legal and Compliance, including:

- i. written opinions and interpretations on legal basis, consent, notice and cross-border matters
- ii. applicability assessments for new products, processes and partnerships
- iii. support on grievances, escalations and proceedings before the Data Protection Board

Final decisions and regulatory submissions remain the Bank's prerogative

15. Training Programme, Delivery & Effectiveness. Prepare the privacy training and awareness calendar and programme for DPO approval. Deliver role-based training to:

- i. The Board and senior management
- ii. The DPO office, Legal, Compliance, IT, DBD and CISO
- iii. Business units and branch staff
- iv. Contractual and outsourced staff

- v. Deliver refreshers on every material regulatory change, and additional sessions, workshops or presentations to any forum (Board, regulators, auditors, business units) as required. Measure and report coverage and effectiveness through attendance, assessment scores and behavioural indicators.

16. Awareness Campaigns & Content. Run enterprise awareness campaigns. Produce regularly updated content, such as posters, presentations, questionnaires, mailers, intranet content, short videos, podcasts, comics and newsletters, in the languages required by the Bank.

17. Drills & Simulation Exercises. Conduct table-top breach drills and simulated Data Principal Rights and grievance exercises. Report outcomes with remediation actions and track them to closure.

7.1.4 System Integrator (Technical Implementation) Responsibilities

1. **Procure, Implement and operationalise DPDP Solution Suite** - a comprehensive end-to-end solution as per industry's best practices ensuring full compliance with the DPDP Act, DPDP Rules across all modules.
2. Configure and deploy a **Consent Management Platform (CMP)** integrated with all customer-facing digital and assisted channels (internet banking, mobile app, website, IVR, chatbot, branch/CSR systems...), capturing a logs-based (immutable) consent artefact with purpose, timestamp, version, channel and IP address, and propagating consent status and DPRM rights with downstream to all consuming systems and processors in real time/near real time.
3. Implement **data discovery and classification** to identify, tag and map personal and sensitive personal data across structured and unstructured repositories, including legacy, archived, cloud and SaaS data stores, with scheduled re-scans and automated ROPA/inventory refresh, automated notifications to designated team, data custodian/steward in case of any meta data changes in incremental scan along with meta data versioning.
4. Build and integrate **automated DPR/ Consent workflows** access, correction, completion, updation, erasure, nomination, consent withdrawal and grievance redressal with identity verification, defined SLAs, escalation matrices, dashboards and full immutable audit trails.
5. Implement automated retention, archival and certified erasure workflows per the Bank's retention schedules and statutory overrides, with erasure certificates and propagation to backups, archives, DR copies and processors.
6. Deploy and integrate **breach detection, logging, alerting and notification** capability able to meet statutory and regulatory breach-reporting, RBI, CERT-In and the DPB, with breach register and evidence capture.
7. Implement **age-gating and verifiable parental/guardian consent** mechanisms for children's data and for persons with disability having a lawful guardian.

8. Integrate all DPDP technical controls with the Bank's IT and security infrastructure i.e. AD, IAM, DLP, encryption/key management, PIM/PAM, SIEM, SOAR, ITSM, GRC, CRM, UEBA, Grievance Module, ticketing etc without **disruption to core banking operations**.
9. Prepare HLD, LLD and FSD for every module (on-premises and cloud), API/integration specifications, network and security architecture diagram; maintain under version control with an Architecture Decision Record for every material change.
10. Perform application tiering and a **risk-based integration plan** across the full **250+** applications; adopt API-first integration by default, batch/file integration for legacy or high-volume systems, and manual/compensating controls with documented Bank risk acceptance for the residual set; maintain a single **Application Integration Tracker**.
11. Build out and size all environments (Dev/SIT/UAT /Prod/DR) on-premises and in cloud in line with Bank IT and Cloud policies; use masked/synthetic data in non-production environments.
12. Harden OS, database, middleware configuration to Bank baselines with hardening-checklist sign-off mandatory before every environment promotion.
13. Implement encryption at rest and in transit, tokenisation/masking of sensitive fields, Role Based Access Control, least privilege and privileged-access management for all privacy-technology components.
14. Conduct **UAT, SIT, regression, performance/load testing against Non-Functional Requirements, VAPT and secure code review** prior to go-live of every DPDP-related component and at least annually thereafter; close all critical and high findings before production release and obtain Bank sign-off.
15. Onboard all privacy-technology log sources to SIEM, tune use-cases and alerts with respect to DPDP suite and other in scope Software Solutions.
16. Establish **DR/BCP** for all privacy-technology components with replication, defined and validated RTO/RPO, and full DR drill with documented report.
17. Provide ongoing **patching, version upgrades, Hardening, VAPT and change-management support** to keep technical controls aligned with evolving DPDP Rules and Bank baselines.
18. Ensure open standards and interoperability, avoidance of vendor lock-in, licence sizing adequate for the Bank's growth in users, data volume and applications, and source-code/configuration escrow where applicable.
19. Embed Privacy-by-Design and Privacy-by-Default gates in the SDLC for all new applications and changes enterprise-wide;

7.1.5 Compliance of Audit Observations

1. Conduct mock audits and readiness assessments ahead of any scheduled internal, statutory or regulatory audit.

2. Plan the remediation strategy and execution thereof for compliance of audits observation covering policy adherence, consent records, DPR request handling, retention and erasure logs, breach handling and vendor compliance.
3. Align DPDP audits with the Bank's existing audit processes (CSITE, RBI, IS Audit, and others) in coordination with Internal Audit, Risk, Compliance and Information Security.
4. Track closure of prior audit observations and maintain an open-items and action-tracker register.

7.1.6 Acceptance and Sign-off

1. Each deliverable shall be submitted with bank defined acceptance criteria; the Bank shall provide written acceptance or return-with-comments within an agreed turnaround.
2. Sign-off on a deliverable shall be a prerequisite for the corresponding payment milestone.
3. Dedicated sign-off certificates shall be issued for go-live of each component, stabilisation exit, DR drill completion, VAPT closure, and each DPIA cycle.

7.1.7 Integration Approach & Responsibilities

1. The Bidder shall study the Bank's existing Enterprise Architecture and deploy the DPDP Solution Suite to fit within the Bank's Enterprise Architecture, integrating about 250 applications across the Bank, its subsidiaries and the GIFT City IBU through the Bank's existing ESB/API gateway, IAM and SIEM. It shall cover the full consent lifecycle and Data Principal rights under the DPDP Act and Rules. International Financial Services Centres (IFSC) data flows shall follow International Financial Services Centres Authority (IFSCA) and RBI norms, and the design shall be approved by the Bank's Architecture team.
2. The Bidder shall conduct walkthrough meetings with upstream and downstream application teams on the solution and the changes required for integration. The same support shall be extended to the Bank's application OEMs, service providers and partners.
3. The Bidder shall prepare the Functional Specification Document and related documentation covering the integration approach, the list of APIs to be developed by the downstream/ upstream applications with effort estimates, and a developer toolkit (API specifications, SDK/connector guides, sample code and a test sandbox). All documents require the Bank's approval before build starts. The upstream/ downstream application integration scope should be clearly defined.
4. The Bidder shall customise the DPDP Solution Suite wherever required and develop the required API connectors, SDKs etc for upstream/downstream application which will be further routed through API Gateway, ESB, middleware etc as needed for seamless integration with the Bank's applications.

5. The Bidder shall implement real-time propagation of Consent and Rights decisions from the Consent Management Platform to downstream applications, with retry and failure handling; and periodic reconciliation between the Platform and each application, with automated exception reports/dashboard and a remediation workflow visible to the DPO.
6. The Bidder shall drive integration through Dev/SIT/UAT deployment, test case design and execution (including regression and performance testing), VAPT closure, sign-off by the Business owner and DPO, and production rollout.

7.2 The DPDP Suite — Detailed Technical & Functional Requirements

7.2.1 Notice & Consent Management

1. **Customer Consent Master Data Management Layer:**

The Bank requires a Customer Consent MDM layer as the Single Source of Truth (SSOT) for all consent records. The bidder shall either demonstrate that this capability exists within the DPDP Suite or build/customise for the Bank. The same can be leveraged by the facility of Data Warehouse.

The layer shall capture every consent action (grant, update, amendment, withdrawal) and propagate it in real time, through APIs, to all linked upstream and downstream applications. This keeps consent status consistent across the Bank's systems.

Responsibilities are divided as follows:

- a. **Consultant:** design the Consent MDM layer, covering the data model, integration architecture and propagation logic.
- b. **System Integrator (SI):** implement, integrate and test the layer as per that design
2. Provide mechanisms for single, comprehensive, broken and granular consent at the Unique Customer Identification Code (UCIC) and account level, ensuring purpose specific consent management as per DPDP Act & Rules.
3. Enable explicit consent **collection, storage, and retrieval**.
4. Allow users to set **granular preferences** for specific purposes such as data sharing, marketing communications...
5. Determine the **applicability of each legitimate use** with regards to personal data processing activities undertaken by the Bank across each product, processes, and internal business function.
6. Solution must seamlessly integrate with the Consent Managers registered and approved by DPBI via secure, real-time APIs to validate, log, and dynamically enforce data processing consents in strict compliance with the **Digital Personal Data Protection (DPDP) Act**.
7. Integrate **identified legitimate** uses and purposes with the Bank's overall Privacy Management Framework.
8. Support for incorporating **consent templates based on business** requirements.
9. Implement **digitally verifiable parental/guardian consent mechanisms** for minors, in accordance with the DPDP Act.
10. **Design, collect and manage consents as per DPDP Act ,2023** and other relevant

regulatory requirements for ex. Reserve Bank of India (RBI), Insurance Regulatory & Development Authority of India (IRDAI), UIDAI.

11. Support **hierarchical consent** structures based on user attributes, data categories, and processing purposes.
12. Maintain detailed **consent records** including timestamp, purpose, and data shared.
13. Consent **revocation tracking** and enforcement
14. **Collection, storage, Renewal, revocation, logs, security (immutability)**, and auditability.
15. Coverage across **digital, physical, and hybrid (phygital)** journeys.
16. Centralized repository for managing user consents.
17. Maintain an **audit trail** of consent records, including timestamps, purposes, associated processing activities as required under DPDP Act 2023.
18. Ensure that consent artefacts are immutable, admissible in court, and meet regulatory standards as per MeitY's / DPDP Consent Framework.
19. Implement **consent retention and expiration** mechanisms as per legal and regulatory requirements.
20. Trigger necessary communications (email/SMS/WhatsApp/in-app) for expired/ expiring consent.
21. 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.
22. Ability to generate customizable & dynamic notices tailored to different products and journeys.
23. Provide **downloadable consent** receipts/artefacts for transparency.
24. Ensure translation and transliteration of **notices into all 22 Indian languages**.
25. Provide banking options (logos & themes) to relate with the Bank's language design.
26. Maintain **version control for all notices** generated within the user journey.
27. Record and store multiple versions of consent agreements and maintain historical consent changes for audits.
28. Audit trail for all consent related activities and same cannot be altered
29. Ensure **identification and notification of Data Principals who consented to outdated versions**.
30. Integrate seamlessly with third-party systems/Consent Management Platform to **centralize consent records** and ensure consistency across platforms.
31. Maintain a centralized repository for consents collected via **third-party platforms**.
32. Enable **syncing of updated consent** records with internal and external systems.
33. Platform must support **multi-device and multi-channel** consent synchronization across web, app, kiosk, chatbot and future digital interfaces to ensure consistency and compliance across all user touch points.
34. Ensure WCAG 2.1-AA compliance for notice and interactions
35. Consent Management platform to be integrated with all downstream/ upstream applications using API, SDK/connector...
36. Enterprise wide consent repository capability (single system of record) that stores

consent including consent purpose, timestamp, consent status (active/revoked), and reference to notice provided...

37. Customers accessible journeys/ platform enabling reviewing, modifying, and withdrawing consents (Option across Mobile Banking/ Internet Banking, Digital journeys, other customer touchpoints) and propagate status changes to all relevant systems (AA layer, Digi Locker integration, underwriting/ eligibility workflows, CRM/analytics... where applicable) within a defined SLA
38. Proactive notification to customers of material changes affecting consent (e.g., change in purpose of processing, data categories collected, third-party sharing/recipients, retention period, or consent terms) and to obtain fresh/re-confirmed consent
39. Automated Workflows where consent revocation/ modification for services take effect within defined timelines (e.g., immediate/T+1 for digital channels) across all relevant systems, remove/mask/anonymize consent-captured attributes from single source of truth and derived stores (data marts...) where legal/regulatory retention does not require keeping it. Confirmation & audit logs to record the same
40. System to handle exceptions (wrong consent mapping, consent disputes, failed revocation propagation) and link to grievance handling system within defined timelines
41. Stop processing for withdrawn consent purpose i.e. a) cease processing consent-dependent data for that purpose within a defined timelines (e.g., profiling/ personalization...) b) suppresses the customer from outbound campaigns across SMS, WhatsApp, email, app push, and outbound calls

7.2.2 Cookie Management

1. Auto-Scanning of sub-folders and sub-domains of the website and extracting cookies.
2. Granular consent options (per category, per purpose, or per service).
3. Autoblocking of cookies, including 3rd party scripts and tags, based on consent provided by the user.
4. Customizable banner template and compliance with WCAG 2.1-AA
5. Dynamic cookie consent banner aligned with DPDP Act, RBI advisories and other regulatory requirements.
6. Auto-translation of cookie banner content into 22 languages as mandated by the DPDP Act.

7.2.3 Data Principal Rights Management (DPRM)

1. Provide a portal for Data Principals to view and manage their consents.
2. Allow Data Principals to download a copy of their consent history.
3. Enable mechanisms for Data Principals to exercise all rights under the DPDP Act, including:
 - a. Right to access consent
 - b. Right to revoke consent

- c. Right to correction and erasure of data (Clause 12), including third-party workflow integration
- d. Right to grievance redressal
- e. Right to nominate a representative in the event of death or incapacity, including the ability to appoint, modify, or revoke a nominee, and enable nominees to access, withdraw, or erase data as permitted
4. Implement efficient workflows to receive, process, and respond to Data Principal Requests within the Bank.
5. Orchestrate SMS, email, WhatsApp, and in-app notifications to Data Principals through communication gateways, Mobile Banking, and Internet Banking.
6. Support self-service handling of consent view and revoke requests to minimize tickets for the privacy team or DPO office.
7. Facilitate orchestration of data deletion requests between the Fiduciary and Data Processors.
8. Enable service agents to verify consent artifacts, locate relevant personal data related to deletion requests, and take appropriate action.
9. Maintain a centralized register/tracker to record all Data Principal Requests, responses, and resolution times, demonstrating compliance.
10. Securely log and track all requests to support audits, verification, and regulatory reporting.
11. Provide a dedicated grievance portal/ integrate with Bank's existing grievance system with intake through web, mobile application, branch, call center, e-mail, chatbot, WhatsApp and physical channels
12. Design, implement and operate an enterprise-wide grievance system to receive, process, track, escalate, resolve and report privacy-related grievances in accordance with the Act, the Rules and Bank policy

7.2.4 Third Party Risk Management

1. Create, assign Third party risk assessments to vendors and manage the lifecycle.
2. Establish a centralized **Third-Party Risk Management (TPRM) framework** to monitor, assess, and mitigate risks arising from vendors, service providers, and outsourcing partners that process personal data on behalf of the Bank.
3. Ensure **comprehensive compliance** with the **Digital Personal Data Protection (DPDP) Act, 2023**, covering obligations such as consent validation, data minimization, breach notification, and **lawful processing by third parties**.
4. Create a **centralized vendor inventory** capturing detailed information about all third parties handling personal or sensitive data, including the nature of services, data types processed, and processing locations.
5. Enable vendor classification and risk segmentation based on multiple parameters such as **data sensitivity, processing volume, access level**, and business criticality (e.g., high, medium, low risk tiers).
6. Facilitate risk scoring, workflow automation, and escalation for **high-risk or non-compliant vendors**, including automated notifications and corrective action

tracking.

7. Implement continuous monitoring dashboards to provide real-time visibility into third-party compliance posture, key risk indicators, and audit results.
8. Provide incident and breach management workflows, including third-party breach reporting, escalation, root-cause analysis, and remediation tracking.
9. Incorporate cross-border data transfer validation mechanisms to assess adequacy, consent, and notification requirements for vendors located outside India, as per DPDP Act provisions.
10. Maintain a **comprehensive audit trail of all vendor risk assessments**, approvals, remediation actions, and compliance status changes for regulatory and internal audits.
11. Include **periodic review mechanisms** to reassess vendor risks based on contract renewals, scope changes, or compliance incidents.
12. Provide reporting and analytics features, including trend analysis, vendor risk heatmaps, and performance dashboard.
13. Support data lifecycle management by tracking personal data shared with vendors, ensuring secure transfer, storage, and deletion as per retention schedules.
14. Ensure role-based access controls (RBAC) and secure authentication mechanisms for authorized stakeholders managing third-party risk data.
15. Deliver configurable templates and policy frameworks for third-party onboarding, assessment, and compliance certification.
16. Support regulatory reporting and readiness by maintaining evidence of third-party compliance aligned with DPDP obligations and sectoral guidelines.

7.2.5 Personal Data Discovery & Data Security Posture Managements

1. **Manage, organize and discover personal data** across both structured and unstructured sources.
2. Ensure seamless **cataloging of personal data** across cloud platforms and on-premises systems.
3. Provide comprehensive support for **unstructured files, relational databases, and data warehouses**.
4. Monitor and track personal data lineage across internal systems as well as external third parties.
5. Generate **visual lineage diagrams** to illustrate the flow of data.
6. Automatically detect, classify, and tag personal data of children (under 18 years) and individuals requiring guardian consent, including persons with disabilities.
7. Accurately **identify and classify sensitive data elements**, with special emphasis on Indian PII, across all data types.
8. Support unstructured data formats such as PDF, Images, XLSX, DOCX, any other file containing PI Data
9. Scan and classify all data assets to detect Indian personal data fields, including names, Aadhaar, PAN, and Driving License documents...etc.
10. Identify historical versions of Indian-specific identifiers, including Aadhaar, PAN,

- Voter ID, and Driving License, across all states.
11. Tag personal data within the organization-wide data dictionary for centralized tracking.
 12. Catalog and classify endpoint devices for complete coverage.
 13. **Support multiple operating systems**, including Windows 8 through the latest Windows versions, MacOS, Linux, and Ubuntu.
 14. Enable **unified management** of endpoints through mobile device management.
 15. Provide capabilities to define and **enforce policies for endpoint devices**.
 16. Maintain a structured inventory of personal data to support governance and compliance requirements.
 17. Capture and store metadata for each data element, including creation date, modification history, data owner, classification, and sensitivity level.
 18. Integrate the data dictionary with **automated assessments** to streamline compliance processes.
 19. Facilitate oversight of third-party processors managing PII data, including cross-border transfers and data retention checks, to trigger necessary compliance assessments.

7.2.6 Record of Processing Activities (RoPA)/ Data Protection Impact Assessment (DPIA)

1. Provide **standardized templates and workflows** for conducting DPIAs, covering detailed descriptions of processing activities, including third-party involvement.
2. Include a **risk assessment matrix** to evaluate potential risks, with automated risk calculation and categorization by product and process with respect to DPDP Act.
3. Offer regulatory- and **industry-specific DPIA templates** that can be customized to meet organizational needs.
4. Enable **multi-level workflow functionality** to support role-based access, permissions, and approval processes.
5. Allow **customization of roles, permissions, and review procedures** to align with organizational structures and governance policies.
6. Support automated reminders, query escalation, and follow-ups to streamline DPIA completion.
7. Provide functionality to upload supporting documents and artefacts in response to specific queries.
8. Support periodic **DPIA reviews to maintain** ongoing compliance with regulatory requirements.
9. Proactively initiate assessments for new business processes, with a timeline view to ensure accountability and visibility.
10. Enable **secure and seamless sharing of DPIA assessments** with data processors and vendors to ensure end-to-end compliance.
11. Allow addition of team members and external stakeholders for collaborative assessment activities.

12. **Leverage AI to auto-fill assessments** using a knowledge base of consent artefacts, processors, configurations, and data discovery findings.
13. DFD (Data Flow Diagram) tool for visual representation of Data flow for the processes.
14. Prepare detailed **Data Flow Analysis Document/Report** to cover/capture all the processes followed in the respective department/office. The document should also capture all the journeys related to handling of PII/sensitive data in the department like:
 - Data ingress and egress points
 - Data handling, storage and sharing mechanisms.
 - Data access rights/privileges.
15. Identify the details of data storage in the department/branch which includes Understanding the various endpoints and review mechanism used to store the received and processed data for e.g., Data stored in local systems, data stored on file servers, etc. along with recording and analyzing the type of data being stored.
16. Reviewing all the process involved and analyzing the risks associated with the security of data in transit, use and at rest with respect to DPDP Act.
17. Establish a systematic approach for classifying and mapping data, creating an inventory to understand the types of data the Bank processes.
18. Assist the Bank in implementing measures for secure storage, retrieval, and disposal of sensitive information.
19. Implement a centralized ROPA repository covering all applications, systems, products, processes, departments, branches, business functions, and third-party vendors processing personal data.
20. Capture purpose of processing, categories of Data Principals, personal data categories, recipients, processors, transfers, retention periods, lawful basis, consent linkage, security controls, and processing ownership.
21. Integrate ROPA with Consent Management, DPIA, Data Discovery, Data Catalogue, Vendor Risk, and Breach Management systems.
22. Enable automated DPIA triggers for high-risk or materially changed processing activities.
23. Provide attestation workflows, periodic review, maker-checker approval, DPO review, immutable audit logs, and DPBI-ready export packs.
24. Generate management dashboards for incomplete ROPA records, overdue attestations, high-risk processing, retention gaps, cross-border flows, and processor dependencies.
25. Maintain a living RoPA covering purpose, legal basis, data categories, data principals...and the entries to auto-populate from discovery and lineage outputs including manual data entry.
26. Periodic attestation workflow requiring the business owner to confirm or correct each RoPA entry, with reminders and overdue tracking.
27. Versioned change history with delta reporting and an automatic trigger into DPIA or threat-model reassessment on material change.

28. Every RoPA entry shall be linked to the applicable notice version, consent purpose, DPIA and threat model.
29. Each RoPA entry shall identify the processors and sub-processors involved and the contract governing the transfer and Regulator-ready RoPA export in CSV and PDF, filtered by business unit, purpose or data category.

7.2.7 Data Breach & Incident Management

1. Implement **breach investigation and notification workflows** that comply with the requirements of the DPDP Act and associated rules.
2. Maintain a repository of pre-approved templates for rapid and compliant breach reporting.
3. Document and display steps taken to contain and remediate breaches, ensuring transparency and trust.
4. Generate and notify **initial and final breach reports to both impacted Data Principals, Data Protection Office and the Data Protection Board**.
5. Maintain a comprehensive audit trail of all breach-related actions to demonstrate regulatory compliance.
6. Segment and create cohorts of affected Data Principals to ensure notifications are sent only to those impacted.
7. Support **automated breach notifications** to impacted Data Principals within the timeframes defined by the DPDP Act and rules.
8. Provide **configurable templates for breach intimation**, ensuring clarity, accuracy, and regulatory compliance.
9. Suggest **remedies to impacted Data Principals** to mitigate risks.
10. Show steps taken to contain the breach, ensuring transparency and trust.

7.2.8 Privacy Enhancing Technology (Data Encryption, Masking, Tokenization and Anonymization)

1. Implement encryption of personal data at rest across databases, file systems, endpoints, backups, archives, cloud storage and other repositories.
2. Implement encryption of personal data in transit using secure protocols across internal networks, APIs, mobile applications, internet-facing systems and third-party integrations.
3. Provide dynamic data masking for production environments and static data masking for non-production, analytics, training, testing and development environments.
4. Support tokenisation, format-preserving encryption, pseudonymisation, anonymisation and field-level protection for Aadhaar, PAN, account numbers, card data, contact details, authentication data and financial fields.
5. Integrate with HSM/KMS, IAM/PAM, SIEM/SOC, DLP, Data Discovery and Classification tools.

6. Provide key rotation, segregation of duties, decryption approval, secure key recovery, audit logs for encryption/decryption/masking events, and real-time alerts for suspicious access.
7. Deploy a PET-enabled privacy management capability for automated consent tracking, purpose enforcement, data minimisation, privacy monitoring and privacy-risk detection.
8. Support PET techniques such as anonymisation, pseudonymisation, differential privacy, homomorphic encryption, federated learning and privacy-preserving analytics where applicable.
9. Embed PET controls into analytics, AI/ML pipelines, data science sandboxes, reporting environments, data exchange workflows and high-risk processing use cases.
10. Implement purpose binding, minimization rules, over-collection detection, re-identification risk checks and auto-fail controls where thresholds are breached.
11. Integrate with Consent Management, ROPA, Data Catalogue, DPIA, GRC, ITSM, Third-Party Risk, Analytics and SIEM/SOC systems.
12. Maintain tamper-evident logs and audit exports showing PET mechanism used, applied parameters, risk thresholds, exceptions, approvals and compliance evidence.

7.2.9 Privacy Threat Modelling

1. Adopt a structured privacy threat modelling methodology such as LINDDUN (**Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of information, Unawareness, and Non-compliance**) or an equivalent Bank-approved framework tailored to BFSI use cases.
2. Model privacy threats across data collection, storage, processing, analytics, sharing, retention and deletion stages.
3. Cover threats including unauthorized access, insider misuse, third-party leakage, excessive exposure, profiling, inference risks, purpose violation and rights-fulfilment exposure risks.
4. Integrate threat modelling into SDLC, DevSecOps, change management, product approval and technology enhancement processes.
5. Generate privacy threat registers, severity ratings, mitigation recommendations, residual-risk status, owner assignments and DPIA-ready exports.
6. Provide customized dashboards for DPO, DPO office and Executives showing privacy threat posture, open mitigations, overdue actions and high-risk journeys.

7.2.10 Privacy Training Awareness

1. Design/Review a **comprehensive training and awareness program** that will help the Bank to drive privacy-first culture across the organisation.

2. This should include but not be limited to, Training sessions (**online/ offline**), broadcast messages, Quiz, Privacy Comics Table top exercise, Mock drills etc., on a Quarterly basis/on-demand during the contract period.
3. Conduct **role-based privacy training** (staff, IT, customer care, vendors etc.)
4. Design awareness campaigns (newsletter, mailers, posters, quizzes, e-learning, QR Based, Podcasts...).
5. Deliver annual training package with segment-specific curriculum.
6. Enterprise level customizable dashboard and Reporting as per the Bank requirement (for Data Protection Board, DPO department and Senior management).
7. Audit log maintenance to **demonstrate compliance and provide a verifiable trail** of training activities, data processing activities during audits or breach investigations.

7.2.11 Dashboards and Reporting, Audit Logs

1. Enterprise level customizable dashboards and Reporting as per the Bank requirement (for Data Protection Board, DPO department and Senior management).
2. Dashboard in Mobile Banking/ Internet Banking other digital touchpoints for the Customer to view active consents across Digi Locker/ Account Aggregator...etc, showing purpose, consent status (active/revoked..), validity..etc , modify/withdraw these consents and confirmation (reference ID with updated status visible to the customer..).
3. Dashboard and Reporting functionalities for the DPO department/ Bank to check the requests raised by customers asking the bank to access, correct, delete, restrict, manage personal data and consents along with the count of bank's customers who gave consent, Count of DPR requests received and resolved in certain period range, average response time....
4. Audit log maintenance to **demonstrate compliance and provide a verifiable trail** of training activities, data processing activities during audits or breach investigations.
5. **Reports**-The bidder shall provide up to 100 reports as specified by the Bank. The Bank will define each report's content, format and frequency during the requirement-gathering phase. The reports shall be available through the DPDP Suite with export to Excel, PDF, CSV etc . Reports shall be scheduled or on-demand, as specified.

7.3 Non- Functional Requirements

The following requirements shall form an integral part of the Scope of Work and shall apply in addition to the module-specific requirements stated elsewhere in this RFP.

1. **Deployment Architecture:** The complete suite shall be deployed in the Bank's UAT, Pre-Prod, Data Centre and Disaster Recovery environments with high availability, no single point of failure, synchronized configuration,

automated failover and the capability to operate in active-passive mode and, where required, active-active mode.

2. **Licensing and Capacity:** Licenses shall cover all modules, components, connectors, APIs, agents, management consoles, upgrades and support required for the contract period. Data Discovery and Classification shall be sized for up to 20000 endpoint/user licenses or the final quantity specified in the Bill of Material, whichever is higher.
3. **Onsite Support:** The bidder shall provide resources at onsite during implementation and, from go-live as per the resource section in the RFP for operations and support in shifts. Equivalent substitutes shall be provided during leave, attrition or replacement without interruption to services.
4. **Delivery and Integration Milestones:** Installation, configuration, integration and go-live of all modules at UAT, Pre-Prod, DC and DR shall be completed within timelines as defined in RFP. Application integration shall be executed in approved phased lots and completed within the overall implementation period.
5. **Availability and Performance:** The solution shall be designed for 99.99% availability, high-volume concurrent API requests, encrypted backup and restoration, defined RTO/RPO, regular DR drills and performance monitoring without material degradation of integrated applications.
6. The solution must be deployed in PSB's **On-Premises Data Centre and DR** site and ensuring compliance with banks policy.

7.4 Functional and Technical Requirements questionnaire.

The solution's functional and technical requirements questionnaire are detailed in Appendix-1.

7.5 Other requirements

1. The Bidder to note that all the requirements pertaining to Requirement analysis, System design, Development & Installation, Documentation, Deployment, and Go-live of the enterprise data privacy solution are to be performed by the bidder in active consultation with the OEM.
2. The Bank will provide the necessary hardware **Virtual servers** (Windows/ RHEL/ Ubuntu) on VMware VCF, SAN NVMe storage, S3 Storage, Network components - VLAN/ IP, Switch, Rack, Ports, AVI Load balancer, Backup infrastructure, Database (Oracle ULA) based on the sizing requirements submitted by the bidder for the Data Center (DC) and Disaster Recovery (DR) sites. The bidder shall provide the exact sizing of the underlying infrastructure strictly based on the details and data volume metrics mentioned in Appendix 2 of this RFP.
3. The design should ensure high availability within the primary site incorporating failovers, automated database backups, and system health monitoring—while also including a robust disaster recovery plan with a secondary site that meets

the defined availability requirements stated in the RFP. The proposal must include detailed architecture diagrams, data flow maps, and a clear sizing justification.

4. The bidder should arrive at the sizing independently in concurrence with the OEM and same will be shared with the bank for DPDP Suite Implementation. Furthermore, during the contract period, the projected organic customer growth, account volume, and transaction scaling of the Bank must be fully factored in. Thus, the data privacy applications, database discovery engines, and underlying IT infrastructure proposed should have sufficient CPUs, memory, storage, NICs, and ports available to accommodate the predicted data mapping, consent tracking, SLAs, and processing requirements of the Bank. The solution/appliances proposed must feature adequate vertical headroom to manage scaling volumes of Data Principals without performance degradation.
5. In addition to the Core Data Privacy & Consent Management modules, the bidder will provide an enterprise-grade solution for high-availability database replication between the DC and DR sites. It shall be the sole responsibility of the bidder to supply, install, configure, manage, and maintain the replication engine to ensure zero data loss (RPO=0) of consent tokens, audit trails, and privacy compliance logs.
6. Any requirements from the Bank for customization, enhancement, and system administration required in the supplied solutions to deliver seamless, fully functional integration—including custom and native data discovery connectors (i.e. core Banking, CRM, cloud databases, etc in scope applications), consent orchestration workflows, Data Principal right fulfilment desks, incident/breach management workflows, alert fine-tuning, notifications, regulatory reporting dashboards, and customization of localized privacy notice templates—shall be undertaken by the bidder during the Contract period. This condition holds true even in the case of an extension of timelines for the final commissioning and go-live of the DPDP suite due to any reason, and any such extension would be at the sole discretion of the Bank.
7. It is hereby clarified that the DPDP Suite deployment is an enterprise-wide regulatory implementation. If there is any regulatory changes by DPBI /RBI before Go Live of solution the same shall be delivered by bidder
8. The Bidder must provide, maintain, and regularly update a comprehensive Software Bill of Materials (SBOM), CBOM for the privacy suite, explicitly detailing all open-source libraries, encryption dependencies, and compliance modules up to the last level to verify the security integrity of the privacy platform.
9. Necessary operational services over and above this, such as deployment, platform management, and regulatory SLA adherence, will be the sole responsibility of the bidder. The PSB expects bidders to optimally size and factor in data processing pipelines in compliance with the RFP requirements. However, if at the time of implementation there is a structural shortfall or non-compliance of any module, component, hardware, or software required for the full operational functioning of the bidder's proposed DPDP compliance platform

10. The bidder shall install, configure, and commission the required data privacy software components, encryption frameworks, and data scanning modules into the designated infrastructure to build functional production, testing, and staging environments.
11. The bidder shall be responsible for providing all application-level event logs, user access trails, system state alerts, and required data processing telemetry from the privacy platform, ensuring its seamless integration with the Bank's centralized Security Operations Center (SOC) and enterprise SIEM tools for real-time security monitoring.
12. The bidder shall position a dedicated technical team consisting of **consultant Lead, OEM Resource, L1 and L2** data privacy support resources to implement, commission, and manage the proposed setup under a managed services model, ensuring strict compliance with the Digital Personal Data Protection Act, MeitY guidelines, RBI information security mandates, and other regulatory or statutory frameworks issued from time to time.
13. The AI solution and underlying system (if used in DPDP solution suite/ any supporting module) must strictly adhere to the regulatory frameworks, advisories, and circulars issued by the Ministry of Electronics and Information Technology (MeitY) (including IT Intermediary Guidelines and AI Advisories) and the Reserve Bank of India (RBI) (including but not limited to RBI Model Risk Management principles, Master Directions on IT/Cyber- security Governance, and the FREE-AI Framework).
14. For Generative AI / Large Language Models (LLMs), the Bidder must implement strict Retrieval-Augmented Generation (RAG) guardrails, input/output validation, and programmatic filters to prevent hallucinations, prompt injection, jail- breaking, and data leakage. The bidder shall conduct algorithmic bias, fairness, and sensitivity audits to ensure the AI system delivers non-discriminatory outputs across diverse demographics
15. The AI solution (if used) must incorporate a **Human-in-the-Loop (HITL) or Human-on-the-Loop** mechanism for critical and sensitive decision workflows. The Bidder must provide administrative controls that include an instantaneous "Kill Switch" / Deactivation mechanism, allowing authorized Bank's administrators to immediately disable the AI engine or fall back to rule-based/manual operations in the event of anomalous drift, model degradation, or safety breaches.
16. The bidder shall deliver an explainable AI (XAI) architecture, interpretable audit trails detailing the rationale, confidence scores, and data inputs that contributed to every automated inference or recommendation. Full technical documentation, including model cards, architecture diagrams, benchmark validation results, model lineage, and hyper- parameter logs, must be provided for independent internal/external audits and RBI supervisory review.

7.5.1 Training

All technical product training must be provided directly by the OEM and the bidder. The bidder should submit a comprehensive readiness plan to the Bank highlighting

the levels of training required before deploying any personnel on the DPDP platform operations.

Training needs to be organized covering the following core modules:

- a) Administrative Training : new platform features, creation of compliance dashboards, setting of privacy risk indicators, data inventory metrics, MIS reporting, regulatory alert and data breach incident management, data lineage/lifecycle analysis, data discovery scanning engine configuration, consent orchestration workflows, functional changes made to the system baseline, automated rights fulfilment, industry best practices, and changing DPDP/regulatory trends.
 - i. Submit Training Calendar to be approved by bank
 - ii. Advanced architectural study material, regulatory compliance Sops etc
 - iii. Training needs to be organized post Go-Live, and thereafter at least once every year or immediately after major framework updates or new regulatory compliance features are released
 - iv. Maintain Logs of Meeting
- b) Privacy Awareness Training : Employees awareness, Business units, Third Party/Vendors, Top management , etc
- c) Run enterprise awareness campaigns and updated content like (posters, Presentations, Questionnaire, Tests, mailers, intranet content, short videos, Podcast, Comics, newsletters etc)
 - i. The bidder must submit training calendar.
 - ii. The bidder must deliver 4 distinct training sessions per year .
 - iii. Comprehensive Updated study material, official documentation, must be provided. The Bank shall provide the required physical infrastructure for any training sessions conducted at the Bank's premises.
 - iv. Maintain Logs or records of training provided as per DPDP act or rules compliance

7.6 Annual Technical Support (ATS)

1. Bidder should provide software licenses with comprehensive on-site ATS for the entire contract duration.
2. Rates provided by the bidder for the respective software, hardware and services shall be used on a pro-rata basis for any additional software, hardware and/or services utilized by the Bank during the contract period.
3. ATS must comply with the Technical Standards, Security Requirements, Operating Procedures and Recovery Procedures
4. Acceptance Test: - Bank may carry out the acceptance tests for testing of Data Protection Suite, verification that the supplied components are as per bill of material through Bank or Bank appointed third party auditor. The Bidder shall assist Bank in all acceptance tests to be carried out by Bank. This test ensure that the Data Protection Suite is compliant with RFP terms and conditions.

5. Solution Go-Live and final sign-off: - The final sign off shall be provided by the Bank after complete installation and implementation of all the components as per the Purchase Order and to the satisfaction of the Bank. License period shall start from the date of Go live of Solution.
6. Bidder should provide comprehensive Support for all software products OS, etc., as applicable. Bidder is required to install upgrades, new releases and handle the faults/problems at no extra cost to Bank during the entire contract period.
7. The Total ATS charges applicable after Go-Live shall be not less than forty-five percent (45%) of the Total License cost quoted by the Bidder. The Annual Technical Support charges shall not be less than fifteen percent (15%) of the Total License cost quoted by the Bidder.

7.7 Resource Requirement

S.No	Resource Type	Deployment	Count	Shifts (Minimum)	Experience/Skillset
1	Project Manager SPOC	– Onsite	1	As per PSB timings and calendar.	• B.E./ B.Tech in CS/ IT/ ECE, MCA • At least one certification in Project management like PMP, CIPM/ CIPP. • Minimum 6 years of overall experience, out of which at least 2 years in data privacy/DPDP related projects. • Strong knowledge of project management/implementation management of data protection/security solutions. • Should have experience of managing at least 1 privacy solution implementation .

S.No	Resource Type	Deployment	Count	Shifts (Minimum)	Experience/Skillset
2	SME / Legal / Lead - L3	Onsite	1	As per PSB timings and calendar.	• LLB/LLM or B.E./B.Tech/MCA with specialization in Cyber Law/Data Protection • DCP/ DCDPO/ CIPM/ CIPP certified (or equivalent Data Protection certification) • Minimum 5 years of experience in data privacy, IT law, or regulatory compliance • Working knowledge of the DPDP Act 2023 and related frameworks (GDPR etc.) • Experience advising on at least 1 data protection/privacy implementation for a PSU/PSE/Govt. Department/BFSI organization
3	DevOps / API - L2	Onsite	2	As per PSB timings and calendar (shift basis).	• B.E./B.Tech/MCA in Computer Science/IT/ ECE • Minimum 4 years of experience in application support, DevOps and API integration (CI/CD, containerization,...) • Relevant certification preferred • Hands-on experience with API management/ integration for privacy/ security solutions
4	L1 Support Engineer	Onsite	4	24x7 rotational shifts as per PSB requirement.	• B.E./B.Tech/BCA/B.Sc in Computer Science/IT • Minimum 2 years of experience in application/technical support • Familiarity with incident management and ticketing tools (ServiceNow/ITSM) • Basic understanding of data protection/DPDP requirements • Incident Management
5	Data Privacy / DPDP Consultant	Onsite	1	As per bank requirement	• Graduate or Postgraduate in Law / IT / Information Security / Risk Management with any of following Certification • Minimum 5+ years of experience in data privacy and protection frameworks, including hands-on experience in privacy gap assessments, policy and SOP drafting, DPIA / PIA,

S.No	Resource Type	Deployment	Count	Shifts (Minimum)	Experience/Skillset
					consent management, and regulatory advisory under DPDP, GDPR, or other equivalent privacy regulations for BFSI / regulated entities.
6	Information Security & Privacy Architect	Onsite	1	As per bank requirement	- B.E./ B. Tech/ MTech in Computer Science / IT / Cyber Security with with any of following Certification CISA /CISSP /CIPP / CIPM / DCDPO / CDPSE / ISO/IEC 27001 LI/LA - Minimum 3+ years of experience in information security and privacy-by- design, including implementation or advisory experience related to data protection controls, encryption, access management, logging, monitoring, and security safeguards, aligned to DPDP, ISO/IEC 27001, or RBI cyber security guidelines.
7	DPIA / ROPA/Privacy Risk Assessment Specialist	Onsite	1	As per bank requirement	- Graduate or Postgraduate in Law / Risk Management / IT / Information Security with any of following Certification CIPP / CIPM / DCDPO / CDPSE 5+ years of experience in conducting Data Protection Impact Assessments (DPIA) / Privacy Impact Assessments (PIA), privacy risk assessments, threat modelling, and definition of mitigation controls for BFSI or large enterprises under DPDP, GDPR, or similar privacy regulations.

Total Resources: 11

7.7.1 Roles & Responsibilities

1. Project Manager (PM) - Duties

- Act as single point of contact (SPOC) for the Bank/client for all project-related matters.
- Plan, schedule, and track overall project execution, milestones, and deliverables as per the DPDP compliance roadmap.

- Coordinate between the Bank, the implementation team, and third-party vendors/OEMs.
- Prepare and present periodic status reports, presentation decks, risk registers, and escalation matrices to stakeholders.
- Ensure adherence to SLAs, timelines, and quality standards throughout the contract period.
- Own change management, resource allocation, and issue resolution for the engagement.

2. L3 - SME / Legal / Lead - Duties

- Provide subject matter expertise on the DPDP Act 2023 and related regulatory requirements.
- Review and validate data mapping, consent management, and grievance redressal processes for legal compliance.
- Support drafting/reviewing of privacy notices, consent artefacts, and data processing agreements.
- Conduct or support Data Protection Impact Assessments (DPIA) and compliance audits.
- Advise the project team on regulatory changes and their impact on the implementation.
- Lead a team providing technical/functional direction for solution design and rollout.
- Lead in the overall DPDP compliance of the Bank and preparation of the relevant report to the Bank's DPO team.
- Advise the Bank's team in the Grievances related to DPDP or Data Principal Rights requests.

3. L2 - DevOps / API - Duties

- Manage deployment, configuration, and integration of the DPDP solution with existing banking applications via APIs.
- Set up and maintain CI/CD pipelines for solution updates and patches.
- Perform application support, troubleshooting, and root-cause analysis for Level 2 incidents.
- Monitor system performance, availability, and security of integrated components.
- Coordinate with infrastructure/cloud teams for environment provisioning and scaling.
- Escalate unresolved issues to L3/OEM and document resolutions for the knowledge base.

4. L1 – Duties

- Provide first-line support and monitoring for the DPDP solution on a 24x7 basis.
- Log, identify, prioritize, response and resolve basic incidents/service requests within defined SLAs.

- Escalate unresolved or complex issues to L2/L3 support with proper documentation.
- Perform routine health checks, backups, and basic maintenance tasks.
- Maintain incident logs and update tickets in the ITSM tool.
- Support end users with basic queries related to the data privacy/DPDP application.
- Provide first-line support and monitoring for the DPDP solution on a 24x7 basis.

5. Consultant – Duties

- The duties of consultancy are defined in Section 7.1.3.

7.7.2 Duties of Bidder

The bidder is required to provide competent on-site human resources consisting of L1 and L2 PM Lead Consultant and technical personnel. The Bank may require an increase in the on-site personnel resources of the bidder and/or OEMs from time to time; such additional resources must be provisioned within one (1) month from the date of written communication from the Bank. The on-site resources must be provided with adequate guidance, technical assistance, and architectural support by competent off-site Subject Matter Experts (SMEs) of the bidder and OEMs.

1. Each designated operational shift team must include one Team Lead/Shift In-Charge who shall function as an L2 resource.
2. Resources will be required to be positioned in the Data Protection Office, DC, DR, or any other office location based strictly on the Bank's requirements.
3. The Bidder shall be responsible for meeting all SLA requirements for the proposed data privacy solution and managed services, including the provision of any additional resources required for the same at no extra cost. In case the Bank requires additional manpower for compliance activities not covered under the core scope of this RFP, the Bank reserves the right to obtain such resources from the Bidder on a pro-rata basis, at the exact same rates quoted in Appendix 2: Commercial Bill of Material.
4. Shift Operations: The DPDP compliance, consent management tracking, and privacy breach monitoring ecosystem will function as a 24x7x365 operational environment. Personnel resources must be capable of working in rotating shifts and flexible working hours to seamlessly support continuous compliance operations, data discovery monitoring, and statutory timelines.
5. The quantity of resources listed in the resource allocation table represents the minimum mandatory baseline required for on-site deployment. Bidders must ensure that their on-site and off-site deployments are appropriately scaled while adhering strictly to these minimum requirements.

6. The deployment of L1 and L2 personnel on-premises must be right-sized across shifts by the bidder to guarantee uninterrupted 24x7 support.
7. The deployed personnel shall be "Named Resources." Arbitrary swapping or changing of resources is strictly prohibited unless explicitly requested by the Bank or under unavoidable circumstances, which shall be governed by the applicable SLAs and require prior written approval from the Bank.
8. In case of resource replacement, a strict transitioning and Knowledge Transfer (KT) period of 30 days must be adhered to. The Bidder must notify the Bank in writing well in advance before initiating any transition or KT period. The cost of the overlapping resource during the KT period shall be borne entirely by the bidder.
9. The Bidder must deploy highly competent resources capable of executing the necessary implementation, configuration, regulatory maintenance, and operational support as per the mandates of the Bank. The Bidder must deploy adequate resources to ensure that the DPDP systems are fully implemented within the specified timelines, remain operational with high availability, and ensure that customer/Banking services are completely unaffected. To guarantee that technical and regulatory SLAs are met, the Bidder shall deploy extra resources during the contract period without any additional cost to the Bank.
10. The Bank reserves the right to interview all personnel resources proposed to be deployed on the project and reject any individual not found suitable for the role.
11. At any later stage of the contract, if any deployed personnel resource is found unsuitable to perform their assigned data privacy/technical duties, or violates any of the Bank's governance, information security, or administrative guidelines, the Bank reserves the right to demand the immediate removal and replacement of such personnel.
12. The Bank's compliance services and operations must always remain immune to individual resource dependencies.
13. The Bidder is strictly required to obtain explicit permission from the Bank in writing before removing any personnel resource from the project.
14. During the implementation rollout, regulatory validation, and other critical go-live stages of the project, the bidder must ensure the active availability of their senior management to guarantee smooth coordination, governance alignment, and strategic resource mapping.
15. The Project Manager (PM) will serve as the exclusive Single Points of Contact (SPOC) for the Bank.
16. On-site resources must conform to the Bank's working days, holiday calendar, and operational hours, or as dynamically decided by the Bank for smooth functional integration.
17. The bidder shall be solely responsible for conducting comprehensive police verification and background checks for all resources prior to onboarding. If required by statutory regulators or the Data Protection Board of India (DPBI),

the Bank may request the supporting documentation, which the bidder shall be obliged to submit immediately.

7.8 Facilities to be Provided by the Bank

Unless otherwise stipulated in the Tender Document, no Facilities (including Reference Documents, Medical facilities, Rooms, Furniture, Transport, Access to IT Services etc.) shall be provided by the Bank to bidder/Contractor at Site. The basic infrastructure facilities like seating will be provided by the bank.

7.9 DR Drill

The bidder is responsible for conducting the DR Drill of in-scope solutions on a regular basis and as per the frequency decided by the Bank in the presence of Bank officials. Coordination with the application team, OEMs and Bank's team, is the responsibility of the bidder to ensure the successful execution of the DR drill. The bidder is required to maintain documentation of the DR Drill and provide suggestions on improving the RTO and RPO of DR drills. The DR Drill report with learnings, outcome of the drill must be submitted to the Bank and same will be subject to the audit by the Bank. The periodic DR Drill plan should be submitted in advance to the Bank for scheduling the same in presence and approval of the Bank.

7.10 DR Setup

The DR setup of DPDP suite & Solution complete replica of DC site. The bidder has to make all arrangements for setting up parallel DC and DR Sites. The bidder has to ensure that DR setup is ready on the date of Go Live of each phase of respective Applications and within the agreed timelines.

7.11 System Recovery

1. In case of disaster, it is the responsibility of the bidder to ensure that services remain unaffected and same is up and running from secondary site (DR) as per RTO and RPO according to Bank policies.
2. It is bidder's responsibility to maintain DC – DR patches, updates & upgrades on continuous basis. Bidder to ensure that scheduled / unscheduled DR drills is conducted on regular basis (Quarterly basis or as defined by Bank). As part of these exercises, bidder to submit compliance / completion of activity reports at the end of the activity.
3. Bidder is responsible for performing DR drills between the proposed primary (DC) & secondary site (DR). Also, bidder to participate and assist Bank in their DR drill (planned & unplanned) and ensure the availability of solution during Bank's drills. During the DR Drills, bidder to ensure that full manpower deployment is made available during the drill.
4. Processes shall be in place to allow for recovery to a disaster recovery hardware platform, and the bidder shall provide Estimates of recovery time.
5. Proposed method of recovering the logical state of the production service, Likely extent of data loss in the event of such recovery being required.

6. The bidder shall prepare along with Bank team at the starting of the project. Following documents will be maintained at the Bank level, the bidder team has to regularly update every month highlighting the updates made in the document with respect to the previous version.
 - a. Disaster Recovery Plan- identifying the operations involved in disaster recovery and the dependencies between these operations.
 - b. Disaster Recovery Procedures- providing step-by-step instructions for the operations identified in the Disaster Recovery Plan.
 - c. Disaster Recovery Test Plan- identifying the steps and resources required to carry out a Disaster Recovery test to validate the Disaster Recovery Plan and Procedures.

7.12 Performance and Scalability

The solution must be able to handle our current and projected user traffic without performance degradation. The solution should have flexibility to accommodate any such requirement arises due to regulatory changes, increase in volumetrics as per industry standards etc

7.13 Non-Exhaustive Clause

The above Scope of work for different functions are not exhaustive and may contain the functions as required by the Bank and as per the official Gazette / notification of the Government of India, DFS, RBI, DPBI, Ministry of Finance and Regulatory authorities etc., as communicated from time to time during the contract. The same shall be applicable for compliance of any Audit observation pointed out by RBI/any other regulatory authority or bodies /internal or external auditor of Bank have during the contract.

7.14 CSITE Undertaking Clause

Submission of undertaking by successful Bidder regarding Data Security Compliance:

1. The vendor to Immediately report of customer-data breaches or cyber security incidents involving customer data to the Bank.
2. The vendor shall report immediately to the Bank regarding any unusual cyber incident occurring at the infrastructure of Vendors, Partners, or TPSPs that impacts their operations.
3. The vendor to ensure for prohibiting storage of sensitive customer (Bank's customers) data in plain text and enforce encryption/masking across all technology layers and logs.
4. The SLA should state the liability of the Service Provider in the event of a breach of security or confidentiality and the Service Provider's obligation to inform the Bank. • Data Localization (Circular: DPSS.CO.OD.No 2785/06.08.005/ 2017- 18 dated April 06, 2018):

5. The Service Provider shall notify the Bank's designated incident contacts of any actual or suspected cyber security incident or personal data breach immediately and in any event within one (1) hour of discovery. The initial notification shall not be delayed for want of complete information.
6. Further, the Successful Bidder shall immediately contain and mitigate the incident by preserve all logs, forensic evidence and other relevant records
7. The Successful Bidder shall undertake root-cause analysis and provide periodic incident updates at intervals specified by the Bank and provide all information and assistance required by the Bank for reporting to RBI, CERT-In, Data Protection Board of India or any other competent authority;
8. The Successful Bidder shall not make any communication, notification or public statement concerning the incident without prior written approval of the Bank, except where disclosure is mandatorily required by law; and
9. The Successful Bidder shall bear all reasonable costs incurred by the Bank for containment, investigation, remediation, forensic examination and regulatory response to the extent attributable to the Successful Bidder or its personnel/sub-processors.
10. The Service Provider shall provide updates at the frequency directed by the Bank and all information required to enable the Bank to meet statutory and regulatory reporting timelines, including the seventy-two-hour timeline under the DPDP Rules where applicable.
11. Service Provider shall ensure all data processed by processors must be stored only at locations within India expressly approved in writing by the Bank, in accordance with applicable RBI directions. Any transfer or processing of personal data outside India shall require the Bank's prior written approval and shall comply with the DPDP Act, the DPDP Rules, applicable RBI directions and any restriction or order issued by the Central Government or a competent regulator. The Service Provider shall maintain an up-to-date data-location register and shall ensure the same obligations apply to every approved sub-processor.

7.15 Exit Plan Management

1. The scope of work mentioned is illustrative and not exhaustive. Bidder needs to comply with the Bank's requirements and any statutory or regulatory guideline(s).
2. Bidder to provide Termination/Expiration Assistance regardless of the reason for termination or expiration
3. Bidder to comply/adhere to the Exit Plan
4. Bidder will not make any changes to the Services under the Agreement and continue to provide all Services to comply with the defined Service Levels.
5. Bidder to perform reverse transition of services to the Bank's new vendor or Bank's officials.
6. Bidder shall within ninety (90) days of the Signing Date, deliver to Bank a plan specifying the Termination/Expiration Assistance including functions and services of Bidder necessary to accomplish the transfer of responsibility of the Services

from the Bidder to the Bank or a Third Party. In the event of Term Expiration or termination of this Agreement, the plan shall at minimum, contain Bidder's detailed plan for Operational and Knowledge Transfer requirements and list of documentations.

7. The Exit Plan shall be updated by the Bidder on an annual basis in accordance with Bank's requirements and delivered to Bank for its approval on or before the start of each Contract Year.
8. Knowledge Transfer and Handover of Services
9. Bidder to provide transfer of knowledge with respect to Services
10. Provide Bank's personnel or designated third party personnel training for the Services that are to be transferred.
11. Bidder shall train Bank's designated personnel and/or its designee(s) for any process or associated Equipment's', Materials, Systems or tools used in connection to the Services
12. Provide Bank and/or its designee(s) information regarding Services (as necessary) for implementation of the Exit Plan. Bidder to also provide information regarding Services as reasonably necessary to the Bank or its designee(s) to overtake responsibility for continued performance of Services in an orderly manner to minimize disruption in operations.
13. Provide Bank or its designee(s) a complete copy of the Bank's IP that are in Bidder's possession and Bidder's IP that Bank is licensed or otherwise authorized to use.
14. Explain the change management process, problem management process, Policies and Procedure Manual, reports and other standards and procedures to Bank's or its designated staff.
15. Provide technical documentation for Software used by the Service Provider for continued Services
16. Identify, record and provide release levels of Software and update of records of release levels prior to and/or during transition of Services
17. Provide assistance to the Bank or its designated officials for notifying the third-party vendors for procedures to be followed during the transition of Services.
18. Ensure transfer of Configuration Management Database (CMDB) that contains details of data elements that are used for management of Services. The CMDB must be in a form that can be migrated to a new environment that can manage Configured Items.
19. Bidder shall provide other technical and process related assistance, as requested by the Bank.
20. The bidder will not be allowed to take Bank's IP information.
21. The Vendor shall cooperate fully with both the Bank and new service provider(s) to ensure there is a smooth transition. The Vendor shall not erase, purge, revoke, alter or change any data during the transition period, unless specifically advised by the regulator / Bank Bidder is required to provide the data dictionaries and data in the requested format to the Bank/Banks identified bidders.

7.16 Security Management

1. Authentication and authorization mechanisms for all users and systems should ensure enforcing bank's security policies.
2. End to end security mechanism to ensure security of logs, data, information, alerts, users, configurations etc. at rest / storage / database, during processing and in transit.
3. User Id and login should determine level of access to data e.g. read/view data, print data, write/modify data, delete data etc.
4. The solution should support the following security features:
 - a) Username and password for accessing the applications and database
 - b) Access credentials should not be stored on the endpoints
 - c) Auto blocking/locking of applications access upon reaching maximum number of tries. The maximum number of incorrect errors should be defined by the Bank.
5. Termination of session and log off after lapses of configurable time.
6. The solution should support the following transaction level security:
 - a) End-to-End encryption of data transmission (symmetric or asymmetric)
 - b) The solution should support multiple authentication-based Bank's preferences
7. The solution should support the following platform security & reliability:
 - a) Data stored is encrypted in the platform database
 - b) Audit trails and logging features must be available in Web Server, application server and database server
 - c) Ability to assign specific rights to platform administrators for secure and restricted access
 - d) Solution should have the ability to support external certifying authority
 - e) The solution should have secure interfaces to various hosts systems according to prevailing security standards
 - f) Application access credentials should not be stored locally.
 - g) Solution should support standard algorithms like AES
 - h) Solution should have a minimum encryption strength of 256 bit for end-to-end transaction (Standard encryption algorithms like 3DES, AES, PKI scheme, with minimum encryption strength of 256 bit)
 - i) The predefined pages of the web portal should handle web application security threats like Cross-site scripting, SQL injection flaws, Malicious file execution, Information leakage, Improper error handling, Broken authentication and session management, Insecure Cryptographic storage, Failure to restrict URL access.
 - j) Platform should have a clear separation of security responsibilities and should be designed for externalized security implementing JAAS (Java Authentication and Authorization Services) allows for pluggable providers
 - k) OWASP Top 10 Compliant

- l) Password must be hashed by SHA256 at least and include Salt or using salt supported cryptography
- m) All the sensitive data (e.g. passwords), including their backups, stored in an encoded or encrypted form in order not to be readable in case of exploitation or other application corruption
- n) Sensitive Data Exposure:
 - i. Sensitive data should be masked when output.
 - ii. Sensitive data should not be stored in source code, config files and logs.
 - iii. Passwords are hashed using Salt.
- o) Configurable approval rules set up for Bank administrator to perform the actions
- p) Regulatory & Statutory:
 - i. The solution should comply with the security principles and practices as stipulated by Statutory and regulatory authorities in India
- q) Application:
 - i. OS Security check up. Application should have capability to detect if the application is running on a jail-broken / rooted / malware infected device.
 - ii. Application must prevent hackers from accessing the application in a case where the device is rooted or jail broken.
 - iii. Blacklisting/Blocking of older versions of the Application on the back end, if there is a security breach.
- r) Transaction Logs:
 - i. Should maintain detailed transaction logs to enable processing audit trails to be reconstructed in the event of any disputes or errors
 - ii. The storage and retention period of logs should be parameterized
 - iii. Security safeguards should also be implemented to protect the information from unauthorized modification or destruction
 - iv. System should facilitate maintaining logs.
 - v. Provision to generate detailed reports, logs, audit trails

7.17 Escrow

The Bank and the Bidder shall agree to appoint an escrow agent to provide escrow mechanism for the deposit of the source code of any customization done on Commercial off the shelf software products supplied/ procured by the Bidder to the Bank in order to protect its interests in an eventual situation. The Bank and the Bidder shall enter into a tripartite escrow agreement with the designated escrow agent, which will set out, inter alia, the events of the release of the source code and the obligations of the escrow agent. Costs for the Escrow will be borne by the Bidder. The escrow agreement shall require periodic deposit of complete, current and buildable source code, build instructions, dependencies, documentation and encryption keys necessary for continuity. Release events shall include insolvency, cessation of support, material uncured breach, prolonged service disruption, termination for bidder default and failure to meet end-of-support obligations. The Bank shall receive a perpetual license to use

released materials solely to operate, maintain and transition the solution for its internal business and regulatory purposes.

8 CONTRACT PERIOD

1. The Contract shall comprise, in descending order of precedence: (a) the executed Contract/SLA and its schedules; (b) the Letter of Award/Purchase Order; (c) corrigenda and written clarifications issued by the Bank; (d) this RFP and its appendices/annexures; and (e) the selected bidder's accepted bid. Any bidder term, disclaimer, exception or qualification not expressly accepted in writing by the Bank shall have no effect.
2. The Bidder is required to sign the contract within 30 days from the date of acceptance of the Purchase Order.
3. The Contract Period shall comprise the Implementation Period stated in the **Project Timelines (i.e. 20 weeks)** plus a support, operations and maintenance **period of three (3) years commencing** on the date of successful Go-Live and written acceptance by the Bank. Obligations intended to apply before Go-Live, including mobilisation, implementation, confidentiality, security, audit and compliance obligations, shall apply from the Effective Date of the Contract.
4. The Bank may, at its sole discretion and subject to satisfactory performance, extend the contract for an additional period of two (2) additional years, in one-year incremental tranches. Unless otherwise agreed by the Bank after price discovery or negotiation, during the extension period, the annual rates of the respective support components shall not exceed 15 – 20% of the last year's support component (ATS / Services) prices and no extension shall become effective unless confirmed in writing by the Bank.
5. The decision to further extend the contract with the same Bidder shall be at the sole discretion of the Bank.
6. Further, the Bank will have the right to renegotiate the prices of ATS rates at the end of the contract period.

8.1 End of Sales / End of Support

1. The Bidder must ensure that any equipment (hardware / software) supplied as part of this RFP has neither reached nor announced end of sales on the date of such supply and has not reached end of support for at least the duration of the contract (including the period of the two-year extension).
2. In the event that any equipment supplied by the Bidder reaches end of support within the contract period, the Bidder shall replace the equipment / component at no additional cost to the Bank.
3. During the extension period, if any product goes end of support, the Bidder is required to provide extended OEM support for the proposed product, or provide the Bank with an alternative product of similar or higher configuration from the OEM (with requisite support), at no additional cost to the Bank.

8.2 Pre-Contract Integrity Pact

The Pre-Contract Integrity Pact Agreement submitted by the Bidder during bid submission will automatically form a part of the Contract Agreement till the conclusion of the contract, including the extended period

8.3 SBOM/CBOM:

Software Bill of Materials (SBOM)/ Cryptographic Bill of Materials (CBOM)

- i) Software Bill of Materials (SBOM): Bidder must provide a comprehensive SBOM that includes complete list of software components, libraries, dependencies, frameworks, and version details included in the source code.
- ii) Cryptographic Bill of Materials (CBOM): The bidder must submit a detailed CBOM comprising detailed inventory of all cryptographic components used, including algorithms, libraries, certificates, key lengths, protocols, and configurations.

9 PROJECT TIMELINES

The Bidder shall complete implementation of all modules in a phased manner as indicated below, within an overall implementation window of 20 weeks from contract signing/effective date, followed by stabilisation, hypercare and steady-state **3-year Operations & Maintenance**.

Overall Implementation shall be done within the contract period, in a phased manner as per below. Complete implementation has to be completed within 20 Weeks.

Delivery and Installation Schedule DC & DR

Area	Supply & Design	Build & Compliance	Integrate & Go-Live
Deliverables	• Delivery of licenses, OS and all other Middleware for setting up the complete suite at UAT, DC and DR. Documentation — HLD etc. • Programme mobilisation and governance charter. DPDP applicability and scoping note. Data discovery plan,	• Implementation, installation and configuration of all modules / functionalities of the Data Protection Suite at UAT, DC and DR, including FSD documentation. Configuration of discovery, classification, DLP, consent, retention and RoPA / DPIA modules. • Completion of GAP assessment, RoPA and DPIA. Retention schedule and statutory	• Integration and Go-Live of the complete solution including DC and DR as per RFP with both upstream/downstream applications e.g. CBS, DWH, LOS / LMS, AD, SIEM, Digital Banking Channels and 250+ applications. DR drill and failover validation. • SOP rollout. Compliance

Area	Supply & Design	Build & Compliance	Integrate & Go-Live
	Enterprise Architecture (pre and post CMP). Commencement of GAP assessment etc	override matrix. Consent purpose taxonomy. Processor inventory and vendor risk-tiering framework. Breach response and Board-intimation protocol. <i>Discovery and RoPA outputs to be delivered by Week 6 to feed SI configuration.</i>	validation against RoPA / DPIA findings. Consent notice and Data Principal rights workflow sign-off. Grievance redressal within the 90-day statutory limit. Data Processor contract remediation. Staff and branch training.
	The above is an indicative phase-wise summary only; the detailed scope shall be as per the Scope of Work in this RFP.		
Timeline	Within 2 weeks from the date of Purchase Order	Within 8 weeks from the date of Purchase Order	Within 20 weeks from the date of Purchase Order

*The timelines provided are indicative, but the overall implementation period is non-negotiable. Individual milestones will be discussed and agreed upon with the Bank, and the approved dates will be used for tracking progress and calculating SLAs and LDs

* The above is a high-level scope the detailed deliverables will be as per the scope of work.

The above phasing is indicative; the Bidder shall submit a detailed, resource-loaded project plan (Gantt/PERT) with the Technical Bid, subject to the Bank's review and mutual finalization at the Kickoff stage., followed by ATS/AMC for the remaining Contract Period.

10 EVALUATION CRITERIA

10.1 Preliminary Scrutiny

1. The Bank will examine the Bids to determine whether they are complete, required formats have been furnished, the documents have been properly signed, and the Bids are generally in order.
2. The Bank may, at its discretion, waive any minor infirmity, non-conformity, or irregularity in a Bid, which does not constitute a material deviation.
3. The Bank will determine the responsiveness of each Bid to the Bidding Document. For the purposes of these Clauses, a responsive Bid is one which conforms to all the terms and conditions of the Bidding Document without material deviations. Deviations from, or objections or reservations to critical provisions, such as those concerning Bid Security, Applicable Law, Bank Guarantee will be deemed to be a material deviation.
4. The Bank's determination of a Bid's responsiveness will be based on the contents of the Bid itself, without recourse to extrinsic evidence. The Bank reserves the right

to evaluate the bids on technical and functional parameters, including possible visits to inspect live site/s of the Bidder and witness demos of the system and verify functionalities, response times, etc.

5. If a Bid is not responsive, it will be rejected by the Bank and may not subsequently be made responsive by the Bidder by correction of the non-conformity.
6. If any information / data / particulars are found to be incorrect, Bank will have the right to disqualify the company, take appropriate action and invoke the performance Bank guarantee/ EMD

A stage bid system is adopted for selection of the bidder:

- Stage 1 – Eligibility and Technical Bid evaluation
- Stage 2 – Commercial Bid Evaluation

During evaluation of the Tenders, the Bank, at its discretion, may ask the Bidder for clarification in respect of its tender. The request for clarification and the response shall be in writing, and no change in the substance of the tender shall be sought, offered, or permitted. The Bank reserves the right to accept or reject any tender in whole or in part without assigning any reason thereof. The decision of the Bank shall be final and binding on all the bidders to this document and the Bank will not entertain any correspondence in this regard.

10.2 Eligibility Evaluation Criteria

Eligibility criteria to be met mandatorily by the bidders:

Sr. No.	Eligibility Criteria	Documents Required
1.	The bidder should be operating in India as a registered company under Companies Act, 2013/1956 or LLP (Limited Liability Partnership) Act 2008 or Partnership firms registered under the Indian Partnership Act, 1932 with registered offices in India, and should be in existence in India for at least the last 5 (five) years as on date of opening of the bid.	Copy of Certificate of Incorporation or Partnership Deed, Copy of Registration Certificate/ GST Registration certificate Copies of all documents listed above should be attested by authorized signatory and must be submitted along with the response
2.	The bidder should have valid PAN and GST Registration in India	Copy of Valid PAN Card, GST Registration Certificates issued by competent authority in India
3.	For MSE and Start-ups: The bidder should have a minimum turnover of INR 15 crore per annum in India for each of the past 3 financial years (i.e. 2023-24 & 2024-25 & 2025-26) along with positive net worth.	CA Certificate mentioning the turnover and net worth for each financial year. and Audited Financial statements (Balance sheet & Profit & Loss statement). The CA certificate provided in this regard should be without any riders or qualification.

Sr. No.	Eligibility Criteria	Documents Required
	For others: The bidder should have a minimum turnover of INR 25 crore per annum in India for each of the past 3 financial years (i.e. 2023-24 & 2024-25 & 2025-26) along with positive net worth.	
4.	The Net Worth of bidder firm should not be negative as on 31/03/2026 and also should have not been eroded by more than 30% (thirty per cent) in the last three years, ending on '31/03/2026'.	The bidder should submit certificate from the Company's Chartered Accountant with UDIN to this effect.
5.	The Bidder/OEM should have supplied, implemented and maintaining digital personal data protection Solution in any one (1) Scheduled Commercial Banks/ PSUs/Government Departments / Public Sector Enterprises/BFSI in India or globally during the last 5 years as on date of RFP.	The bidder has to provide relevant purchase order/work order/engagement letter along with satisfactory reference letter/e-mail from the client confirming the details of the solution implemented/services provided along with Name, Designation, Contact details.
6.	An authorized dealer/distributor/ partner of the proposed Solution	If the bidder is an authorized dealer/ distributor, an authorization letter as per Annexure -23 cum Annexure 7 from their OEM and OSO/ OSD to deal/market their product in India and it should be valid for entire contract period from the date of submission of the bid.
7.	The Bidder shall undertake that the proposed solution / software / licenses to be supplied will be free of malware, free of any obvious bugs and free of any covert channels in the code (of the version of the application being delivered as well as any subsequent versions/ modifications done. Proposed solution must natively support core DPDPA modules as per RFP	Self-Certification from the bidder
8.	Bidders should not have been under debarment/blacklist period for breach of contract/fraud/ corrupt practices/ deficiency in services by any Scheduled Commercial Bank/ Public Sector	The bidder should submit self-declaration on the Company's letter head to this effect.

Sr. No.	Eligibility Criteria	Documents Required
	Undertaking / State or Central Government or their agencies/ departments during last three years as on date of RFP.	
9.	Bank shall follow the public procurement guidelines as stipulated in Order ref: 6/18/2019-PPD Dated 23.07.2020 from Department of Expenditure, Ministry of Finance- Restrictions under Rule 144 (xi) of General Financial Rules 2017. 1. Any bidder from a country which shares a land border with India will be eligible to bid in this tender, only if the bidder is registered with the Competent Authority (DPIIT). Bidder to submit the required certificate along with the technical bid. 2. If clause 1 above is not applicable to any bidder, they shall submit the certificate duly signed by their authorised signatory along with the technical bid.	Either of following as applicable: 1. The certificate for being registered with the Competent Authority (DPIIT) 2. Certificate in format
10.	If the bidder or its subsidiary or its associate or sister company or its holding company has already had an association with Punjab & Sind Bank in the past 5 years or at present as a service provider on any project, then the bidder is required to submit the satisfactory certificate from the bank issued/dated post the issuance of the RFP. Additionally, the Bidder should not have any Service Level Agreement/Contract pending to be signed with the Bank pending for more than 6 months from the date of issue of purchase order	Self-Certification from the bidder along with the satisfactory certificate from PSB (In case of association)
11.	Labor Law Compliance	Self-Certification from the bidder
12.	Integrity Pact	Document on 100 Rs Stamp paper, duly signed and stamped by the authorized signatory.

Sr. No.	Eligibility Criteria	Documents Required
13.	The Bidder and Bidder's parent company (applicable if both are different) should not have been declared Non-Performing Asset (NPA), defaulter in repayment of instalments by any BFSI organization and not undergoing Corporate Insolvency Resolution Process (CIRP), liquidation, or bankruptcy proceedings as on date of submission of the tender, otherwise the bid will not be considered	Self-Declaration letter signed by Authorized Signatory to be submitted.
14.	Non-Disclosure Agreement	Document on 100 Rs Stamp paper, duly signed and stamped by the authorized signatory.
15.	The bidder should support office at NCR/Delhi for 24x7 support.	The Bidder should submit the details viz., address, phone no., email id and contact person Name & Mobile no. etc. with documentary proof
16.	Authorization Certificate - Whether the Bid is authenticated by authorized person.	Bidder to submit a copy of the Board Resolution and the Notarized Power of attorney /Letter of authority if authority is sub delegated as mentioned in Board Resolution and KYC documents evidencing the authority delegated to the authorized signatory.

Note:

1. Attested photocopies of all relevant documents / certificates should be attached as proof in support of the claims made. The bidder should provide relevant additional information wherever required in the eligibility criteria. PSB reserves the right to verify /evaluate the claims made by the Bidder independently. Any decision of PSB in this regard shall be final, conclusive, and binding upon the Bidder.
2. In case of business transfer where bidder has acquired a Business from an entity ("Seller"), work experience credentials of the Seller in relation to the acquired business may be considered.
3. In the case of corporate restructuring the earlier entity's incorporation certificate, financial statements, Credentials, etc. may be considered.
4. Either the bidder on behalf of the Principal/OEM or Principal/OEM itself can bid but both cannot bid simultaneously for the said RFP.
5. The bidder/OEM comply with all applicable CVC guidelines, the General Financial Rules, 2017 and Department of Expenditure instructions, as amended from time

to time including CVC guideline 3 (a, b) circular no. 03/01/12, GFR Rule 16(a) of 2005 and OM of DOE dated 25/07/2016. In a tender, either the duly authorised Indian agent on behalf of the Principal/OEM or Principal/OEM itself can bid but both cannot bid simultaneously. An agent shall not submit bids for more than one Principal/OEM for the same item or product in this tender.

6. If an agent submits a bid on behalf of the principal/OEM, the same agent shall not submit a bid on behalf of another principal/OEM in the same tender for the same item/product.
7. Documentary evidence must be furnished against each of the above criteria along with an index. All documents must be signed by the authorized signatory of the Bidder. Relevant portions in the documents submitted in pursuance of eligibility criteria should be highlighted.
8. When deemed necessary the Evaluation Committee may seek clarification on relevant aspects from the Bidder. However, that would not entitle the Bidder to change or cause any change.
9. Bank reserves the right to conduct reference site visit/ video conference/ voice call with the Client to substantiate the credentials/ copy of PO/ Contract copy/ sign-off submitted by Bidder and/ or OEM. In case the input/ feedback received from the Customer is negative/ unsatisfactory, bank reserves the right to reject the Bid

10.3 Evaluation Process

10.3.1 Stage 1 — Eligibility and Technical Bid Evaluation

Bids shall first be scrutinized for completeness, EMD/Bid Security, and compliance with the mandatory Eligibility Criteria on a pass/fail basis.

Only bidders satisfying all eligibility criteria shall proceed to Technical Evaluation.

Sr. No.	Particulars	Scoring methodology	Max Marks	Documents to be submitted for award of mark
1.	Functional Coverage – DPDPA Scope of Work The proposed solution/platform should support modules listed below (Sr. No. 1–11): a) Notice & Consent Management b) Cookie Management c) Data Principal Rights Management d) Third Party Risk	Compliance Scoring (5 Marks):	5	Self-Declaration by the Bidder/OEM confirming that the proposed solution/platform supports the modules as mentioned in Appendix 1

Sr. No.	Particulars	Scoring methodology	Max Marks	Documents to be submitted for award of mark
	Management e) Personal Data Discovery and Data Security Posture Management f) Records of Processing Activities / Data Protection Impact Assessment g) Data Breach and Incident Management h) Privacy Enhancing Technologies i) Privacy Threat Modelling j) Privacy Training Awareness k) Dashboard and Reporting, Audit Logs			
2.	Implementation Experience (Global / India) <u>The Bidder/OEM must have</u> Number and relevance of privacy governance/DPDPA with at least 4 core modules of the proposed modules implementations completed or in progress, for Scheduled Commercial Banks/ PSUs/Government Departments / Public Sector Enterprises/BFSI in India/Global with ≥ 30 Lakhs Customer Base or equivalent complexity) during last 5 years as on date of RFP.	Project Count-Based Scoring (Max 20 Marks): - • <u>≥ 5 Projects</u> : 20 Marks • <u>3 or 4 Projects</u> : 15 Marks • <u>2 Projects</u> : 12 Marks • <u>1 Project</u> : 8 Marks	20	For each cited project:- Purchase Order / Work Order / Engagement Letter-Completion certificate / Reference letter / Client email reference-Client email from official ID with name, designation, contact number- Project brief mapping to modules.

Sr. No.	Particulars	Scoring methodology	Max Marks	Documents to be submitted for award of mark
3.	Module wise implementation experience (Global/ India) The Bidder/OEM must have experience within the last five years as on date of RFP in implementing or currently implementing modules mentioned across Scheduled Commercial Banks/ PSUs/Government Departments / Public Sector Enterprises/BFSI in India/Global with full adherence to regulatory, operational, and technology requirements.	Module-Wise Scoring (Max 15 Marks): a) Notice & Consent Management - 3 b) Cookie Management - 1 c) Data Principal Rights Management -2 d) Third Party Risk Management -1 e) Personal Data Discovery and Data Security Posture Management - 2 f) Records of Processing Activities / Data Protection Impact Assessment - 1 g) Data Breach and Incident Management -1 h) Privacy Enhancing Technologies -1 i) Privacy Threat Modelling - 1 j) Privacy Training Awareness - 1 k) Dashboard and Reporting , Audit Logs – 1	15	For each cited project:- Purchase Order / Work Order / Engagement Letter- Completion certificate / Reference letter / Client email reference- Client email from official ID with name, designation, contact number- Project brief mapping to modules.
4.	Consultancy experience (Global/ India) The Bidder must have experience within the last five years as on date of RFP in providing consultancy services in Scheduled Commercial Banks/ PSUs/ Government Departments / Public Sector Enterprises/BFSI in India/Global	Count-Based Scoring: - (Max 10 Marks): - • ≥5 Projects: 10 Marks • 3 or 4 Projects: 8 Marks • 2 Projects: 6 Marks (Note: for less than 2 projects, Zero marks)	10	For each cited project:- Purchase Order / Work Order / Engagement Letter- Completion certificate / Reference letter / Client email reference- Client email from official ID with name, designation, contact number- Project brief mapping to modules.

Sr. No.	Particulars	Scoring methodology	Max Marks	Documents to be submitted for award of mark
5.	Competency of Professionals (Project Team Capability) Technical competency of professionals proposed for DPDP implementation (privacy + integration).	Team Competency Scoring (Max 5 Marks): A) Privacy Certifications Any of the Below (Max 3 Marks): I. ≥40% team certified (IAPP - CIPP/E, CIPP/US, CIPP/A, CIPP/C, DCPLA, DCPD etc.,) ISC2 - Systems Security Certified Practitioner (SSCP), Certified Information Systems Security Professional (CISSP), Certified in Governance, Risk and Compliance (CGRC), Certified Secure Software Lifecycle Professional (CSSLP) etc.,) ISACA - Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), Certified in Risk and Information Systems Control (CRISC), Certified in the Governance of Enterprise IT (CGEIT), Certified Data Privacy Solutions Engineer (CDPSE) or equivalent : 3 Marks II. ≥30% < 40% certified: 2 Marks B) Integration & Engineering Skills (Max 2 Marks): I. ≥50% skilled in REST APIs, JSON/XML,	5	CVs of proposed resources- Certification proofs duly verified by the Bidder- Deployment plan & resource matrix- Undertaking on availability as per Bank schedule

Sr. No.	Particulars	Scoring methodology	Max Marks	Documents to be submitted for award of mark
		modern web/mobile tech: 2 marks II. $\geq 40\% < 50\%$ skilled in REST APIs, JSON/XML, modern web/mobile tech: 1 mark		
6.	Bidder's Presentation	Points will be assigned by an internal committee as per Table P-1	35	Presentation to be conducted as per the schedule provided by Bank.
7.	On-Premises Demonstration	Points will be assigned by an internal committee as per Table D-1	10	Demo to be conducted as per the schedule provided by Bank.
Total Maximum Marks			100	

Note: The bidder should score minimum 70% of marks out of 100 marks for qualifying under Technical Evaluation. The bidders qualified under Technical Evaluation will be eligible for commercial opening.

Presentation of proposal:

Punjab and Sind Bank will schedule the presentations and intimate the time and locations to the bidders. Failure of a bidder to complete a scheduled presentation may result in the rejection of that Bidder's proposal.

Table P-1

Sr. No.	Presentation Agenda	Maximum Marks
1.	Understanding of Scope & Bank Requirements: Understanding of Bank context, objectives, target operating model, and current landscape awareness.	3
2.	Relevant Experience & Case Studies: Privacy automation at Scheduled Commercial Banks/ PSUs/Government Departments / Public Sector Enterprises/BFSI in India/Global with ≥ 30 Lakhs Customer Base or equivalent complexity; challenges, approach, outcomes, metrics, testimonials.	7

Sr. No.	Presentation Agenda	Maximum Marks
3.	Technical Approach & Implementation Strategy: Project plan, milestones, go-live plan, risk & mitigation strategy.	10
4.	Solution Architecture: On Prem (DC/DR) deployment architecture, Secure integration Layer (APIs & Connectors)	10
5.	Governance & Compliance : DPDPA governance including consent & purpose limitation, rights handling, accountability, continuous monitoring, and regulatory alignment.	5
Maximum Marks for Presentation		35

Table D-1

Tool demo with at least 1,000 pre-loaded sample entries covering:

Sr. No.	Module	Maximum Marks
1.	Notice & Consent Management	2
2.	Cookie Management	0.5
3.	Data Principal Rights Management	2
4.	Third Party Risk Management	1
5.	Personal Data Discovery and Data Security Posture Management	1
6.	Records of Processing Activities / Data Protection Impact Assessment	1
7.	Data Breach and Incident Management	0.5
8.	Privacy Enhancing Technologies	0.5
9.	Privacy Threat Modelling	0.5
10.	Privacy Training Awareness	0.5
11	Dashboards and Reporting ,Audit Logs	0.5
Maximum Marks for Demo		10

The Bidder should score minimum 70% marks in Technical evaluation criteria to qualify under Technical Proposal evaluation.

Other Conditions:

- When deemed necessary the Tender Evaluation Committee may seek clarification on relevant aspects from the bidder. However, that would not entitle the bidder to change or cause any change.
- Scores for the above individual parameters shall be added to determine the technical scores of the bidders. The bidder with the highest technical score shall be ranked as T1.
- Bank reserves the right to conduct reference site visit/ video conference/ voice call with the Client to substantiate the credentials/ copy of PO/ Contract copy/ sign-off submitted by bidder and/ or OEM. In case the input/ feedback received from the Customer is negative/ unsatisfactory, Bank reserves the right to reject the Bid.
- In case no or only a single vendor qualifies the technical evaluation, in such event, Bank may cancel the tender process and re-tender it in conventional two part bid method as per GeM Rule.

10.3.2 Stage 2 - Commercial Evaluation

Commercial Bids of only the technically qualified bidders (scoring ≥ 70) shall be opened. The Bank shall adopt a Quality-and-Cost Based Selection (QCBS) composite evaluation methodology.

Composite Score = (Technical Score obtained $\div$ Maximum Technical Score) $\times$ 70 + (Lowest Quoted Total Contract Value $\div$ Bidder's Quoted Total Contract Value) $\times$ 30

The Bank reserves the right not to accept the lowest or any bid, and to negotiate commercial terms with the H1 bidder prior to award.

10.3.3 Final Evaluation - Weighted Techno Commercial Evaluation Acceptance of Bid & Signing of Contract

- The Bank shall notify the successful Bidder (H1) in writing through a Letter of Award (LoA).
- The successful Bidder shall, within 30 days of the LoA, submit the Performance Bank Guarantee and execute the Contract Agreement and NDA.

Failure of the successful Bidder to comply with the above within the stipulated time may result in cancellation of the LoA, forfeiture of the EMD, and the Bank may consider award to the next-ranked bidder or re-tender, at its sole discretion.

10.3.3.1 Commercial Evaluation Criteria

The commercial bid of only technically qualified bidders shall be opened. These technically qualified bidders as per technical evaluation process will participate in Commercial evaluation process.

The Commercial offers of only those Bidders, who are short-listed after technical evaluation, would be opened. The format for quoting commercial bid is set in Appendix-2 Commercial Bill of Material. The commercial offer should consist of comprehensive cost for required solution. The bidder must provide detailed cost breakdown, for each category mentioned in the commercial bid.

The Bank will determine whether the Commercial Bids are complete, unqualified and unconditional. Omissions, if any, in costing any item shall not entitle the firm to be compensated and the liability to fulfil its obligations as per the Scope of the RFP within the total quoted price shall be that of the Bidder.

The Commercial Bid (CB) with the lowest value will be awarded a financial score (Sf) of 100 points. The financial scores for all other bids will be calculated using the following formula:

$$Sf = 100 \times CB / F$$

(F = amount of Commercial Bid (Last value quoted/entered by the bidder)).

10.3.3.2 Final Evaluation – Weighted Techno-Commercial Evaluation

The Proposals will be finally ranked according to their combined Technical Score(s) and Financial Score as follows:

$$S = ST \times Tw + SF \times Fw$$

Where S is the combined score, and Tw and Fw are weights assigned to Technical Proposal and Financial Proposal that shall be 0.70 and 0.30 respectively.

ST and SF will be calculated for individual bidders, as per description mentioned in Evaluation Criteria Section respectively.

Bidder with the highest Final score shall be considered for award of the Contract.

For example:

Three bidders, namely A, B and C, participated in the bid process and their technical scores are as below:

$$A=70, B=85, C= 90$$

After converting them into percentile, we get

$$ST \text{ for A} = (70/90) \times 100 = 77.77$$

$$ST \text{ for B} = (85/90) \times 100 = 94.44$$

$$ST \text{ for C} = (90/90) \times 100 = 100$$

The Final prices of the bidders are as under: A= Rs. 8500, B= Rs. 9000, C= Rs. 12000

The final cost quoted by the bidders converted into percentile score shall be as under:

$$SF \text{ for A} = (8500/8500) \times 100 = 100$$

$$SF \text{ for B} = (8500/9000) \times 100 = 94.44$$

$$SF \text{ for C} = (8500/12000) \times 100 = 70.83$$

As the weightage for technical parameter and cost are Tw = 70% and Fw = 30% respectively, the final scores shall be calculated as below:

$$S \text{ for A} = (77.77 \times 0.7) + (100 \times 0.3) = 84.439$$

$$S \text{ for B} = (94.44 \times 0.7) + (94.44 \times 0.3) = 94.44$$

$$S \text{ for C} = (100 \times 0.7) + (70.83 \times 0.3) = 91.25$$

Hence, the offer of 'B' (being highest score) will be considered and the contract shall be awarded B' at Rs. 9000 being the final price quoted by B.

Note:

1. The Bank will at its own discretion decide to either –

- Open commercial bids in front of the bidders after the technical evaluation is complete, and calculate the TCO, Or
- The highest technical bidder shall not automatically qualify for becoming selected bidder and for the award of contract by the Bank.

2. The Successful Applicant shall be the first ranked Applicant (having the highest combined score). The final decision on the successful bidder will be taken by the Bank. The implementation of the project will commence upon acceptance of purchase order and signing of Contract by the selected bidder.
3. If for some reason, the successful bidder fails to execute an agreement within a specified timeline, the Bank reserves the right to award the contract to the next most eligible bidder based on the final evaluation scope of technical evaluation scores and commercial prices quoted.
4. In case of a tie of Total Score between two or more bidders, the Bid with higher technical score would be chosen as the successful Bidder.
5. The Bank will calculate the scores up to two decimal points only. If the third decimal point is greater than .005 the same shall be scaled up else, it shall be scaled down to arrive at two decimal points.

11 PAYMENT TERMS

The payment schedule as under:

Sr. No.	Milestones	Payment Terms	
1	Implementation & Integration Cost	1. Eighty Percent (80%) of the Implementation & Integration Cost shall be released upon successful Go-Live of the solution and written acceptance against the applicable acceptance criteria, test results, security clearances and delivery of all required documentation. 2. The remaining Twenty Percent (20%) of the Implementation & Integration Cost shall be released after completion of three (3) months of stable operations from the date of successful Go-Live, subject to satisfactory performance and written acceptance by the Bank. Payment shall not constitute waiver of any defect, warranty, indemnity or other contractual right.	
2	Enterprise-wide Perpetual Software License Cost	Milestone On successful delivery and installation of the licenses which would be considered delivered once the software is made available for view and review of the bank. The Bidder is required to submit the required to submit the following: • Delivery proof • Installation Proof • Invoice of the Product	Percentage 50 %
		On successful UAT Signoff of the respective product	20%

Sr. No.	Milestones	Payment Terms	
		On successful Go-live of the respective product	30%
3	Annual Technical Support (ATS) Cost	Payment for ATS for the license(s) will be applicable from second year onwards and will be made annually in advance on submission of invoices and upon successful completion of the performance obligations for the previous year / Warranty period	
4	Manpower Cost (Consultancy, Facility Management)	Submission of SLA report and Submission of attendance record/register of Onsite resources on Quarterly basis	Quarterly in arrears
5	Consultancy Services Cost	Milestone	Payment terms
		Submission of required documentation and consultancy services as mentioned in 7.1.3 and sign off from bank's team. The Bank may withhold the amount reasonably attributable to incomplete, defective or rejected deliverables until rectification and acceptance.	Quarterly payment of Annual cost as per BOM

1. TDS on payments will be deducted as applicable.
2. All the payments will be made to bidder electronically in Indian Rupees only. Payment will be made against delivery invoices and challans duly acknowledged by Bank officials. Bidder must submit Service Level Agreement, Penalty report along with the invoices for making payment.
3. Further, the above payments will be released only after submission of Performance Bank Guarantee, signing of SLA (including Dos & Don't) and NDA by Successful Bidder.
4. The Bidder's request(s) for payment shall be made to Bank in writing (Invoice) accompanied by the daily/weekly/monthly reports for which payment is being claimed.
5. All the payments to the Bidder shall be subject to the report of satisfactory accomplishment of the concerned task / performance/ delivery of the Services to the satisfaction of Bank for this purpose.
6. Penalties if any, on account of non-compliance of Service Requirements/ liquidated damages, if any, shall be deducted from the invoice value/ EMD/ PBG amount.
7. Under no circumstances Bank shall be liable to the Successful Bidder and/or its employees/personnel/representatives/agent etc. for direct, indirect, incidental,

consequential, special or exemplary damages arising from termination of the Contract.

8. Bank shall not have any liability whatsoever in case of any third-party claims, demands, suite, actions or other proceedings against the Successful Bidder or any other person engaged by the Successful Bidder during performance of the Service.
9. Bank reserves the rights to dispute/deduct payment/withhold payments/further payment due to the Successful Bidder under the Contract, if the Successful Bidder has not performed or rendered the Services in accordance with the provisions of the Contract which the Bank at its sole discretion adjudge.
10. Successful Bidder shall permit Bank to hold or deduct the amount from invoices, for non-performance or part performance or failure to discharge obligations under the Contract.
11. It is clarified that any payments of the charges made to and received by Successful Bidder personnel shall be considered as a full discharge of Bank's obligations for payment under the Agreement.
12. All out of pocket expenses, travelling, boarding and lodging expenses for the entire Term of this RFP and subsequent agreement is included in the amounts quoted in TCO and the Bidder shall not be entitled to charge any additional costs on account of any items or services or by way of any out-of-pocket expenses, including travel, boarding and lodging.
13. Penalties / liquidated damages, if any, shall be deducted from the invoice value.
14. PROJECT SIGN-OFF: Project sign-off will be given after resolution/closure of all post go-live issues raised within 2 months of go-live of the solution or three months from the go-live of the solution whichever is later.

12 SERVICE LEVELS & PENALTIES

12.1 Service Level Agreement

The successful bidder is bound to comply with the Service Levels described below:

- a. The successful bidder shall have to enter into a "Service Level Agreement" (SLA) encompassing all terms and conditions of this RFP to maintain high platform uptime, process regulatory consent pipelines, and provide both technical and managed onsite services during the entire contract period.
- b. Both the bidder and the OEM will be held mutually responsible for the operational maintenance, compliance configuration, patch management, and fault-free execution of the supplied data privacy infrastructure—including software modules, discovery engines, and interfaces—during the warranty and post-warranty ATS periods.
- c. Any regulatory non-compliance, software bug, or technical glitch identified within the installed platform infrastructure (including discovery applications, back-end

- compliance databases, security containers, and system interfaces) must be attended to on high operational priority and covered under the support parameters.
- d. The bidder must maintain a guaranteed minimum uptime of 99.99% on a monthly basis for all enterprise systems and compliance solutions supplied under this RFP, measured continuously over all calendar hours, excluding only maintenance expressly approved in advance by the Bank, to avoid any administrative delays or business disruptions due to platform breakdowns or degraded processing response times. Planned maintenance shall not excuse failure to meet statutory deadlines, security obligations or agreed business-continuity requirements.
 - e. The bidder shall coordinate with the Bank's ITSM team to configure the SLAs as defined in the RFP and submit the configuration details to the Bank team. If, for any reason, the bidder fails to configure or integrate these with the ITSM solution, the bidder must submit the required reports either manually or through an alternative automated solution.
 - f. Any system disruption, data processing failure, or framework exception may be logged and communicated by the Bank's team via corporate email, phone, toll free number or the designated central ticketing application.
 - g. The operational definitions governing this SLA framework are established as follows:
 - i. "Downtime" shall mean the specific time period for which the core DPDP modules, discovery scanners, or user consent portals are completely unavailable or fail to meet the technical standards specified in the RFP. This strictly excludes scheduled maintenance windows planned in advance with written consent from the Bank, and enterprise network link failures outside the direct control of the bidder.
 - ii. "Incident" refers to any functional abnormality, software exception, or process stall in the data privacy platform/ DPDP solution suite that prevents data masking, dynamic logging, Consent life cycle management or the timely execution of Data Principal Requests (DPR), statutory audits and the modules mentioned in the solution/scope.
 - iii. "Resolution Time" shall mean the absolute time elapsed between an incident being formally reported to the bidder's service desk (via verbal, email, ticketing portal, or SMS communication) and the successful implementation of a permanent fix or regulatory data recovery.
 - h. The baseline calculations for platform availability uptime are structured under the following statutory equations:

$$\text{Uptime} = (\text{Total hours during the month} - \text{Sum of downtime hours during the month}) / \text{Total hours during the month}$$

$$\text{Uptime (\%)} = \text{Uptime} * 100$$

$$\text{Total hours during the month} = \text{Total number of calendar days in the month} \times 24 \text{ hours}$$

- i. For calculation of uptime (penalty), planned/scheduled down time will be exempted. Bank will pay to the bidder after deducting the calculated penalty from the payable amount.
- j. The RPO and RTO service levels for data restoration between the primary Data Center (DC) and Disaster Recovery Site (DRS) will be measured continuously using the Bank's tracking frameworks to verify statutory compliance logs are fully preserved:
- k. Recovery Point Objective (RPO): The maximum acceptable data loss window measured in time. In scope DPDP solution suite and other solutions, critical consent ledgers, Data Principal Request records, breach records and audit records, RPO must equal zero (0).
- l. Recovery Time Objective (RTO): The minimum estimated time required to resume fully functional privacy operations and database compliance scanning after an event of default or disaster.
- m. If any critical software component, security connector, or discovery agent within the enterprise setup falls out of service, the bidder and OEM shall either immediately replace the defective unit (with a new one) or provide a standby, on an immediate basis, not more than 4 hours. Bidder shall maintain a proper inventory of standby components for early resolution of issues.
- n. The bidder must establish continuous synchronization between the primary site and the disaster recovery location, ensuring the platform is structurally ready to support unannounced regulatory audits and seasonal cross-site business continuity drills.
- o. The penalty will be deducted in quarterly FMS/AMC/ATS payment. In case the Bank is unable to adjust penalty in FMS/AMC/ATS payment, the Bank at its discretion may invoke the Performance Bank Guarantee (PBG) to deduct the penalty amount.
- p. If the support services are not provided on 24*7 basis and/or satisfactory services are not provided as sought in the RFP, the Bank with its discretion may reject the proposal/ terminate the contract, without assigning any reason.
- q. The business hours are 8 AM to 10 PM on any calendar day the Bank 's branch is operational.
- r. The bidder should comply with the security and audit standards of the Bank and various regulatory guidelines. For this, the bidder should apply new patches related to OS/ firmware & BIOS updates etc, without any additional cost to the Bank, during the contract period.
- s. For all issues related to the solution supplied by the bidder, RCA (Root Cause Analysis) from the respective OEM to be provided by the bidder within 48 hours. The delay in submission of RCA will lead to penalty Rs. 20000/day

12.2 Penalties

For the purpose of this RFP, the total penalties as per Liquidated Damages & SLA shall be capped at 10% of the Total Contract Value except that this cap shall not restrict the

Bank's rights of termination, risk purchase, indemnity, recovery of direct losses, or remedies arising from fraud, willful misconduct, gross negligence, confidentiality breach, data breach, intellectual-property infringement or violation of applicable law. Upon maximum deduction, Bank reserves the right to terminate the Contract by giving 90 days' notice to the Vendor.

If the bidder fails to Implement solution and/or services within the time period(s) specified in the Delivery Schedule or implementation, the Bank shall, without prejudice to its other remedies under the Contract, deduct from the Contract Price, as liquidated damages, a sum equivalent to 1 percent per week or part thereof of product cost* subject to maximum deduction of 10% of the total contract value, until actual delivery and implementation as per related clauses mentioned in RFP.

*Product cost here defined as the sum of Product's license cost and Product's implementation cost

If the LD due to Implementation of the respective product cost/existing product cost reaches 25% of the implementation cost of the respective product/services, the bidder is required to replace the product/services.

Once the maximum deduction is reached, the Bank may consider termination of the Contract at its discretion.

In the event of Bank agreeing to extend the date of delivery at the request of successful bidder(s), it is a condition precedent that the validity of Bank guarantee shall be extended by further period as required by Bank immediately. Failure to do so will be treated as breach of contract. It is clarified, that if Bank agrees to extend the delivery time and /or implementation timelines, the term of the Contract shall also be extended accordingly and PBG shall be extended till the extended Contract period.

If the Bidder fails to complete the due performance of the contract in accordance with the terms and conditions, the Bank reserves the right either to terminate the contract or to accept performance already made by the Bidder after imposing Penalty on Bidder. Penalty will be calculated on per week basis and on the same Rate as applicable to Liquidated Damages. In case of termination of contract, the Bank reserves the right to recover an amount equal to 10% of the Contract value as Liquidated Damages for non-performance

Penalty and Liquidated Damages are not applicable for reasons attributable to the Bank and Force Majeure. However, it is the responsibility of the Bidder to prove that the delay is attributable to the Bank and Force Majeure. The Bidder shall submit the proof authenticated by the Bidder and Bank's official that the delay is attributed to the Bank and/or Force Majeure along with the bills requesting payment.

a. Penalty due to Downtime or due to performance issues:

Below the expected Turnaround time of any application integrated with the Solution, which may impact Banks business.

After implementation of the complete solution, Penalty will be deducted for partial or complete downtime of the system (software failure) as below. No penalty will be deducted for failure of Hardware provided by Bank.

Table – A (For DC & DR) :

Uptime Percentage (U)	Monthly Penalty Rate
Uptime (%) $\geq 99.99\%$	No Penalty
99.50% $\leq$ Uptime (%) $< 99.99\%$	0.25% of TCO
99.00% $\leq$ Uptime (%) $< 99.50\%$	0.50% of TCO
98.50% $\leq$ Uptime (%) $< 99.00\%$	0.75% of TCO
98.00% $\leq$ Uptime (%) $< 98.50\%$	1.00% of TCO
Below 98.00%	1.00% of TCO + 0.50% of TCO for every additional 0.25% drop

1. **Maximum Penalty Cap:** The maximum monthly liquidated damages are strictly capped at 10% of TCO.
 2. **Right to Terminate:** If the penalty breaches the 10% TCO threshold, the Bank reserves the right to terminate the contract.
 3. SLA will be monitored on Monthly basis.
 4. Penalty due to downtime, during contract period will be deducted from any subsequent payment to be made to the Successful bidder.
 5. Penalty due to downtime, during ATS period will be deducted from ATS and OTS payment.
- b. Penalties/Liquidated Damages for non-performance:** If the selected bidder does not meet the specifications/ terms of the RFP during various tests/ stages, the selected bidder shall rectify the same at bidders cost to comply with the specifications/ terms of the RFP immediately to ensure the committed uptime/ terms, failing which the Bank reserves its right to withhold the payment, impose penalty and invoke the Bank Guarantee/ nullify the contract.
- c. Penalties/liquidated damages for Onsite resources Consultant & System Integrator .:**
1. In case the resource goes on leave/absent, replacements having equivalent or more experience and qualification have to be arranged by the selected bidder to ensure that regular functioning of the solution does not hamper. In case replacements are not arranged with equivalent or higher qualified alternate onsite resources, Bank will pay the proportionate amount for the deployment of the of the qualified resident resources only during the said month. The Bank shall also impose a penalty of 0.5% of the monthly resource cost for the respective Resident resource for each week and part thereof of absence. However, total penalty under

this clause will be limited to 20% on the quarterly Resident resource charges payable to the selected bidder.

2. The selected Bidder shall perform its obligations under the agreement entered into with the Bank, in a professional manner.
3. If any act or failure by the bidder under the agreement results in failure or inoperability of systems and if the Bank has to take corrective actions to ensure functionality of its property, the Bank reserves the right to impose penalty, which may be equal to the cost it incurs or the loss it suffers for such failures.
4. If the Bidder fails to complete the due performance of the contract in accordance with the specification and conditions of the offer document, the Bank reserves the right either to cancel the order or to recover a suitable amount as deemed reasonable as Penalty/ Liquidated Damage for non-performance.
5. Any financial loss to the Bank on account of fraud taking place due to Successful Bidder, its employee or their services provider's negligence shall be recoverable from the Successful Bidder along with damages if any with regard to the Bank's reputation and goodwill.
6. Bank may impose penalty to the extent of damage to its any equipment, if the damage was due to the actions directly attributable to the staff of the Bidder.
7. The liquidated damages/penalties shall be deducted/ recovered by the Bank from any money due or becoming due to the bidder under this purchase contract or may be recovered by invoking of Bank Guarantees or otherwise from bidder or from any other amount payable to the bidder in respect of other Purchase Orders issued under this contract, levying liquidated damages without prejudice to the Bank's right to levy any other penalty where provided for under the contract.
8. All the above Liquidated Damages are independent of each other and are applicable separately to distinct defaults and may operate concurrently. and shall be restricted to 10% of TCO during the contract period.
9. Liquidated Damages is not applicable for the reasons attributable to the Bank and Force Majeure.

13 TERMS AND CONDITIONS

13.1 Assignment & Subcontracting

1. The selected bidder shall not subcontract or permit anyone to perform any of the work, service or other performance required under the contract unless permitted by the Bank in writing.
2. In case any subcontracting is permitted by the Bank, the contracting vendor shall be responsible for all services provided to the Bank regardless of which entity is conducting the operations. The contracting vendor is also responsible for ensuring that the sub-contractor is in compliance with the requirements, obligations, and commitments under the contract.
3. If the Bank undergoes a merger, amalgamation, takeover, consolidation, reconstruction, change of ownership, etc., this tender shall be assigned to the new entity, and such an act shall not affect the rights of the Agency under this tender.

13.2 Delays in the Bidder's Performance

The bidder must strictly adhere to the schedule, as specified in the purchase order, executed for performance of the obligations, arising out of the purchase contract and any delay in completion of the obligations by the Bidder will enable Bank to resort to any or both of the following without prejudice to the other remedies available to the Bank:

- a. Claiming Liquidated Damages.
- b. Termination of the purchase order/ agreement fully or partly and claim liquidated damages.
- c. Execution of Bid Declaration Form / Invoking EMD or Performance Bank Guarantee.

13.3 Jurisdiction

Jurisdiction: It is hereby agreed between the parties that any suit or legal proceedings to enforce the rights of either party under this Agreement shall be instituted and tried by a competent court in the city of Delhi only.

13.4 Dispute Resolution

The Bidder and The Bank shall endeavor their best to amicably settle all disputes arising out of or in connection with the Contract in the following manner:

- a. The Party raising a dispute shall address to the other Party a notice requesting an amicable settlement of the dispute within seven (7) days of receipt of the notice.
- b. The matter will be referred for negotiation between General Manager of The Bank / Purchaser and the Authorized Official of the Bidder. The matter shall then be resolved between them, and the agreed course of action documented within a further period of 15 days.

Notwithstanding the foregoing, if a dispute is not resolved through the negotiations stated above, either Party shall refer it to arbitration by a sole arbitrator mutually appointed by the Parties. If the Parties do not agree on the arbitrator within thirty (30) days of receipt of an arbitration notice, the arbitrator shall be appointed in accordance with Section 11 of the Arbitration and Conciliation Act, 1996. The seat and venue of arbitration shall be New Delhi, India. The proceedings shall be conducted in English in accordance with the Arbitration and Conciliation Act, 1996, as amended or re-enacted from time to time.

The laws applicable to this contract shall be the laws in force in New Delhi, India. The contract shall be governed by and interpreted in accordance with Indian law. The award will be recorded in writing, along with the reasons therefor. The arbitration award shall be final, conclusive and binding upon the Parties. Each Party shall bear the cost of preparing and presenting its case, and the cost of arbitration, including fees and expenses of the arbitrator, shall be shared equally by the Parties unless the award otherwise provides.

Nothing in this Clause prevents either Party from seeking urgent interim or conservatory relief from a court of competent jurisdiction under the Arbitration and Conciliation Act,

1996, or prevents the Bank from exercising contractual remedies that do not require adjudication, including withholding, set-off, invocation of a valid bank guarantee and suspension or termination in accordance with the Contract.

The bidder shall continue work under the Contract during the arbitration proceedings unless otherwise directed in writing by the Bank.

13.5 Notices

Notice or other communications given or required to be given under the contract shall be in writing and shall be faxed/e-mailed followed by hand-delivery with acknowledgement thereof or transmitted by pre-paid registered post or courier.

Any notice or other communication shall be deemed to have been validly given on date of delivery if hand delivered & if sent by registered post than on expiry of seven days from the date of posting.

Publicity

Any publicity by the selected Service Provider in which the name of the Bank is to be used should be done only with the explicit written permission of the Bank.

13.6 Legal Compliance

The successful bidder hereto agrees that it shall comply with all applicable union, state and local laws, ordinances, regulations and codes in performing its obligations hereunder, including the procurement of licenses, permits and certificates and payment of taxes where required. The Successful bidder shall maintain all proper records, particularly but without limitation accounting records, required by any law, code, practice or corporate policy applicable to it from time to time including records, returns and applicable documents under the Labour Legislation

13.7 DPDP Compliance

The successful bidder shall comply with all applicable provisions of the Digital Personal Data Protection Act, 2023 and any rules, regulations, or guidelines issued thereunder while collecting, processing, storing, or handling any personal data in connection with this Agreement. The Successful bidder shall implement appropriate technical and organizational security measures to ensure protection of personal data against unauthorized access, disclosure, alteration, or loss. The successful bidder shall immediately notify the Bank of any actual or suspected data breach involving personal data. The successful bidder shall ensure that personal data is used solely for the purposes of performance of the contract and shall not disclose the same to any third party without prior written consent of the Bank. The successful bidder shall indemnify and hold the Bank harmless against any loss, liability, penalty, or damage arising out of any breach or non-compliance with the Digital Personal Data Protection Act, 2023. Obligations linked to provisions having a future commencement date shall be implemented sufficiently in advance to ensure the Bank is compliant on the applicable commencement date. The successful bidder shall also comply with the Information

Technology Act, 2000, CERT-In directions, applicable RBI directions and the Bank's policies notified to it.

Upon becoming aware of an actual or suspected personal-data breach or security incident affecting Bank data or the Services, the successful bidder shall immediately notify the Bank, provide all information then available, preserve relevant evidence and logs, promptly provide material updates, cooperate with the Bank's investigation and response, and take the containment, remediation and recovery steps directed by the Bank. The successful bidder shall process personal data only on the Bank's instructions and to the extent permissible under the applicable law. The successful bidder shall ensure that each person authorized to process it is bound by confidentiality and security obligations.

1. The successful bidder shall assist the Bank in complying with obligations relating to Data Principal Rights such as access, correction, erasure of data, and grievance redressal under the Act.
2. The successful bidder shall maintain complete records of every processing activity carried out for the Bank, including the instruction relied upon, categories of personal data, purpose, systems and locations, recipients, sub-processors, retention period, access events, transfers, deletion and security controls. Such records and supporting evidence shall be made available to the Bank promptly and in a machine-readable format.
3. The successful bidder shall not engage any sub-contractor or sub-processor for processing personal data without prior written permission of the Bank. Any approved sub-processor shall be bound by the confidentiality and security obligations. The successful bidder remains fully responsible and liable for each sub-processor's acts and omissions, and shall provide the Bank with the current list of approved sub-processors.
4. Approval of a sub-processor shall not relieve the successful bidder of any obligation or liability. Before access to Bank Data is permitted, the successful bidder shall execute a written agreement imposing obligations at least equivalent to the Contract, including data-location, confidentiality, security, incident reporting, audit, regulatory access, return/deletion and exit obligations. The successful bidder shall give advance notice of any proposed change and shall not implement the change if the Bank objects on reasonable security, compliance or operational grounds.
5. Upon termination or expiry of the contract, the successful bidder shall return and/or securely delete all personal data and confirm the same to the Bank. The successful bidder undertakes not to keep this data with its company after the end of this agreement. The return and deletion shall include all copies and, to the extent technically practicable, backup copies held by the Successful Bidder or its sub-processors. The successful bidder shall certify completion in writing on the Bank's request evidencing such return and/or destruction. If retention is strictly required by applicable law, the successful bidder shall identify the retained data and legal basis to the Bank, restrict access and use to that requirement, continue to protect it under this clause, and securely delete it when retention is no longer required.

6. The Bank may require return, migration or deletion of specified data at any time during the Contract where required for legal compliance, risk management or transition. Secure deletion shall follow a recognised standard approved by the Bank, and the destruction certificate shall identify the systems, media, copies, backups and sub-processors covered. Until deletion is completed, all contractual protections and audit rights shall continue.
7. Notwithstanding the return or destruction of Confidential Information / Bank Data / Personal Data, the Successful Bidder, its Personnel and its representatives will continue to be bound by their obligations or confidentiality and other obligations hereunder and as per the applicable law.

13.8 Authorized Signatory

The selected Bidder shall indicate the authorized signatories who can discuss and correspond with the Bank about the obligations under the contract. The selected Bidder shall submit at the time of signing the contract a certified copy of the resolution of their board, authenticated by the company secretary, authorizing an official or officials of the Bidder to discuss, sign agreements/contracts with The Bank, raise invoice and accept payments and also to correspond. The Bidder shall provide proof of signature identification for the above purposes as required by the Bank.

13.9 Confidentiality

This document contains information confidential and proprietary to the Bank. Additionally, the Service Provider will be exposed by virtue of the contracted activities to internal business information of the Bank, affiliates, and/or business partners. The Service Provider must undertake that they shall hold in trust any Information received by them under the RFP/ Contract/Service Level Agreement, and the strictest of confidence shall be maintained in respect of such Information. Disclosure of receipt of any part of the aforementioned information to parties not directly involved in providing the services requested could result in the disqualification of the Service Provider, premature termination of the contract, or legal action against the Service Provider for breach of trust. The information provided / which will be provided is solely for the purpose of undertaking the services effectively.

“Confidential Information” includes all Bank Data, personal data, customer information, security information, credentials, configurations, vulnerabilities, audit material, business information and information received by the Bank under a duty of confidence, whether or not marked confidential. The Service Provider / Successful Bidder / Bidder shall use it only to perform the Contract, disclose it only to authorised personnel with a strict need to know, and protect it with at least the degree of care required under applicable law and the Bank’s notified policies.

No news release, public announcement, or any other reference to this RFP or any program there under shall be made without written consent of Bank. Reproduction of this Agreement, by photographic, electronic, or other means is strictly prohibited.

The Service Provider 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. The Service Provider has also agree to restrict access and disclosure of Information to such of their employees, agents, strictly on a “need to know” basis, to maintain confidentiality of the Information disclosed to them in accordance with this Clause.

Moreover, Service Provider has to submit Non- Disclosure Agreement along with technical bid as per the format provided in this document.

13.10 Indemnity

The bidder agrees to indemnify and keep indemnified the Bank against all losses, damages, costs, charges and expenses incurred or suffered by the Bank due to or on account of any claim for infringement of intellectual property rights.

The bidder agrees to indemnify and keep indemnified the Bank against all losses, damages, costs, charges and expenses incurred or suffered by the Bank due to or on account of any breach of the terms and conditions contained in this RFP or Service Level Agreement to be executed.

The bidder agrees to indemnify and keep indemnified Bank at all times against all claims, demands, actions, costs, expenses (including legal expenses), loss of reputation and suits which may arise or be brought against the Bank, by third parties on account of negligence or failure to fulfil obligations by the selected bidder or its employees/personnel.

All indemnities shall survive notwithstanding expiry or termination of Service Level Agreement and the bidder shall continue to be liable under the indemnities.

The indemnities shall include losses, claims, proceedings, compensation, remediation and restoration costs, regulatory action and penalties to the extent lawfully recoverable, and reasonable legal and professional costs arising from: (a) breach of confidentiality, privacy, data-protection or security obligations; (b) personal data breach or cyber incident attributable to the bidder or its personnel, OEMs or sub-contractors; (c) fraud, wilful misconduct or gross negligence; (d) bodily injury or property damage; (e) violation of applicable law; and (f) employment or tax claims relating to bidder personnel. The Bank shall give reasonable notice of a third-party claim where practicable, but delay shall relieve the bidder only to the extent of material prejudice caused by that delay. No

settlement admitting liability or imposing an obligation on the Bank may be entered without the Bank's prior written consent.

13.11 Make in India

The policy of the Govt. of India to encourage "Make in India" and promote manufacturing and production of goods and services in India, "Public Procurement (Preference to Make in India), Order 2017 and the revised order issued vide GOI, Ministry of Commerce and Industry, Department for Promotion of Industry and Internal trade, vide Order No. P-45021/2/2017-PP (BE-II) dated 19th July 2024 subsequent amendments.

The local supplier at the time of submission of bid shall be required to provide a certificate as per Annexure 19 from the statutory auditor or cost auditor of the company (in the case of companies) or from a practicing cost accountant or practicing chartered accountant (in respect of suppliers other than companies) giving the percentage of local content. The Bank shall follow all the guidelines/ notifications for public procurement.

13.12 Force Majeure

Force Majeure is herein defined as any cause, which is beyond the control of the selected Bidder or The Bank as the case may be which they could not foresee or with a reasonable amount of diligence could not have foreseen and which substantially affect the performance of the contract, such as:-

1. Natural phenomenon, including but not limited to floods, droughts, earthquakes, epidemics and pandemics
2. Acts of any government, including but not limited to war, declared or undeclared priorities, quarantines and embargos
3. Terrorist attack, public unrest in work area
4. Provided either party shall within 10 days from occurrence of such a cause, notify the other in writing of such causes. The Bidder or The Bank shall not be liable for delay in performing his/her obligations resulting from any force Majeure cause as referred to and/or defined above. If a Force Majeure event continues beyond 30 days, the Bank may, by written notice, terminate the affected Services or the Agreement, in whole or in part and all obligations expressed quantitatively shall be calculated as on date of termination. Notwithstanding this, provisions related to indemnity, confidentiality survive termination of the contract. A Force Majeure event excuses performance only to the extent and for the period that it directly prevents the affected obligation, and does not excuse unaffected obligations or the Successful Bidder's duty to mitigate and maintain continuity measures. The Successful Bidder may not rely on its or its subcontractor's lack of funds, staffing or ordinary-course performance failure, or failure to maintain the safeguards and continuity arrangements required by the Contract, as Force Majeure.
5. Unless otherwise directed by the Bank in writing, the Bidder affected by force majeure shall continue to perform the obligations under this agreement, which are

not affected by the force majeure event and shall take such steps as are reasonably necessary to remove the causes resulting in force majeure and to mitigate the effect thereof.

6. As soon as the cause of force majeure has been removed, the Bidder shall notify the Bank and resume the affected activity without delay.
7. Notwithstanding the above, the decision of the Bank shall be final and binding on the Bidder in the event of force majeure.

13.13 Ownership & Retention of Documents:

The Bank shall own the documents prepared by or for the selected Bidder arising out of or in connection with the Contract.

The documents shall become and remain the sole and exclusive property of the Bank and Intellectual Property of such documents shall vest with the Bank. Any document for which the ownership or the Intellectual Property do not vest with the Bank, under law, shall be automatically assigned to the Bank as and when such document is created and the selected bidder agrees to execute all the papers and to perform such other acts as the Bank may deem necessary to secure its rights herein assigned by the successful bidder.

The foregoing assignment shall apply to deliverables, configurations, customisations, documentation and other work product created specifically for the Bank. Each Party shall retain ownership of its pre-existing intellectual property. To the extent any bidder or third-party pre-existing material is embedded in or necessary to use a deliverable, the bidder grants, and shall procure for the Bank, a perpetual, irrevocable, worldwide, royalty-free, transferable licence, with the right to permit use by the Bank's service providers, to use, reproduce, modify, maintain and support that material for the Bank's internal, regulatory, continuity and transition purposes.

Forthwith upon expiry or earlier termination of the Contract and at any other time on demand by The Bank, the Bidder shall deliver to The Bank all documents provided by or originating from The Bank / Purchaser and all documents produced by or from or for the Bidder while performing the Service(s), unless otherwise directed in writing by The Bank.

The selected Bidder shall not, without the prior written consent of The Bank/ Purchaser, store, copy, distribute or retain any such Documents.

The selected Bidder shall preserve all documents provided by or originating from the Bank / Purchaser and all documents produced by or from or for the Bidder in the course of performing the Service(s) in accordance with the legal, statutory, regulatory obligations of the Bank /Purchaser in this regard.

The selected bidder shall maintain adequate insurance throughout the Contract Period, with reputable insurers, covering professional indemnity/errors and omissions, cyber liability and data breach, commercial general liability and statutory employee liabilities,

at limits commensurate with the Contract and risks. Evidence of cover and renewals shall be furnished to the Bank on request; insurance shall not limit the bidder's liability.

13.14 Conflict of Interest

The Bidder shall disclose to the Bank in writing all actual and potential conflicts of interest that exist, arise or may arise (either for the Bidder or the Bidder's team) in the course of performing the Service(s) as soon as practical after it becomes aware of that conflict.

13.15 Signing of Pre-Contract Integrity Pact:

To ensure transparency, equity, and competitiveness and in compliance with the CVC guidelines, this tender shall be covered under the Integrity Pact (IP) policy of the Bank. The pact essentially envisages an agreement between the prospective bidders/vendor(s) and the Bank committing the persons/officials of both the parties, not to exercise any corrupt influence on any aspect of the contract. The format of the agreement is enclosed as Annexure-16 on stamp paper.

The Pre-Contract Integrity Pact Agreement submitted by the bidder during Bid submission will automatically form a part of the Contract Agreement till the conclusion of the contract, including extended period.

13.16 Intellectual Property Indemnity:

In the event of any claim asserted by a third party of infringement of copyright, patent, trademark, industrial design rights, etc., arising from the use of the Goods or any part thereof in India, the Vendor(s) shall act expeditiously to extinguish such claim. If the Vendor(s) fails to comply and the Bank is required to pay compensation to a third party resulting from such infringement, the Vendor(s) shall be responsible for the compensation to the claimant including all expenses, court costs and lawyer fees. The Bank will give notice to the Vendor(s) of such a claim, if it is made, without delay. The Vendor(s) shall indemnify the Bank against all third-party claims. In case of violation / infringement of patent / trademark / copyright / trade secret or industrial design, the Vendor shall after due inspection and testing get the solution redesigned for the Bank, at no extra cost.

13.17 Limitation of Liability

Subject to the express exclusions below, the aggregate liability of the Successful Bidder in connection with this Agreement, in respect of claims, losses, costs or damages arising out of or in connection with this RFP or the Agreement, shall not exceed the total Project Cost. The Bank shall not be liable for indirect, consequential, incidental, special, exemplary or punitive losses, damages or claims, including loss of profit, business or revenue. The successful bidder shall not rely on any exclusion of indirect, consequential or incidental loss to avoid liability for the Bank's reasonable and documented costs of investigation, containment, notification, remediation, restoration, recovery, replacement

or procurement of substitute services arising from the successful bidder's breach, or for any amount expressly recoverable under an indemnity.

The limitations set forth herein shall not apply with respect to:

1. claims that are the subject of indemnification pursuant to infringement of third-party Intellectual Property Right,
2. damage(s) occasioned by the Gross Negligence or Willful Misconduct of Service Provider,
3. damage(s) occasioned by Service Provider for breach of Confidentiality Obligations,
4. Regulatory or statutory fines imposed by a government or Regulatory agency for non-compliance of statutory or regulatory guidelines applicable to the Bank, including the DPDP Act and the DPDP Rules.
5. The settlement amount in the event a claim is settled.
6. The limitation and exclusion of liability shall also not apply to fraud, breach of data-protection or information-security obligations, personal data breach or cyber incident attributable to the successful bidder, breach of audit or regulatory-access obligations, unauthorised use or loss of Bank Data, indemnity obligations, abandonment of services, or amounts recoverable by the Bank through risk purchase. Nothing in this Clause limits liability that cannot lawfully be limited.

“Gross Negligence” means any act or failure to act by a party which was in reckless disregard of or gross indifference to the obligation of the party under this Agreement and which causes injury, damage to life, personal safety, real property, harmful consequences to the other party, which such party knew, or would have known if it was acting as a reasonable person, would result from such act or failure to act for which such Party is legally liable. Notwithstanding the forgoing, Gross Negligence shall not include any action taken in good faith.

“Wilful Misconduct” means any act or failure to act with an intentional disregard of any provision of this Agreement, which a party knew or should have known if it was acting as a reasonable person, which would result in injury, damage to life, personal safety, real property, harmful consequences to the other party, but shall not include any error of judgment or mistake made in good faith.

13.18 Order Cancellation

Bank's Right to terminate the entire/ unexecuted part of the Purchase Order on Convenience

1. The Bank reserves its right to cancel the entire/partial/ unexecuted part of the Purchase Order at any time at its convenience without assigning any reason whatsoever.
2. In the event of termination of the Agreement for the Bank's convenience, bidder shall be entitled to receive payment for the Services rendered (delivered) up to the effective date of termination.

Bank's Right to terminate the entire/ unexecuted part of the Purchase Order on Non-Performance/Default

1. The Bank reserves its right to cancel the entire / unexecuted part of the purchase order at any time by assigning appropriate reasons (after providing a cure period of 30 days and thereafter providing a 30-day notice period). Bank shall serve the notice of termination to the bidder at least 30 days prior to terminate services because of one of more of the following reasons but not limited to –
 - a) Non submission of acceptance of order within 7 days of order.
 - b) Excessive delay in execution of orders placed by the Bank.
 - c) The selected bidder commits a breach of any of the terms and conditions of the bid.
 - d) The bidder goes into liquidation voluntarily or otherwise.
 - e) An attachment is levied or continues to be levied for a period of 7 days upon the effects of the bid.
 - f) The progress made by the selected bidder is found to be unsatisfactory.
 - g) If deductions on account of liquidated Damages/penalties exceeds more than 10% of the total contract price.
 - h) If found blacklisted by any Govt. Department / PSU / other Banks / CERT-In, during contracted period.
 - i) Non satisfactory performance of the Project in terms of affecting the Core Systems of the Bank or the Core Business of the Bank and the functioning of the Branches/Offices of the Bank.
2. No cure period shall be required where the breach is incapable of cure or involves fraud, corruption, willful misconduct, unauthorized disclosure or use of Bank Data, a material cyber security incident, repeated SLA failure, abandonment, insolvency, regulatory prohibition or a circumstance requiring immediate action to protect the Bank, its customers or the financial system. In other cases, the Bank may specify a shorter cure period where reasonably required by the severity or regulatory urgency of the breach.
3. If the Bank decides to cancel the unexecuted part of the purchase order in whole or in part in the event of one or more of the following conditions:
 - a) Delay in delivery of the product installation and Go-Live in the specified period (Implementation Timelines + Cure Period).
 - b) Serious discrepancies are noted in product capability and services.
 - c) Breaches in the terms and conditions of the Order.

Then the Bank shall have the right to recover from the bidder any amounts already paid by the Bank in respect of the product (including respective hardware) and/or services after adjusting for the penalties already levied and recovered by the Bank for that specific product/ service. Further, where the bidder is able to provide satisfactory evidence that the delay or default was not attributable to the bidder, such portion shall be excluded from the scope of recovery.

In such case, the Bank may procure on its discretion, upon such terms and in such manner as it deems appropriate, Hardware, software and services similar to that part of the canceled purchase order, and subject to limitation of liability clause of this RFP. However, bidder shall continue performance of the Contract to the extent not terminated.

4. The Bank reserves its right to invoke the Bank Guarantee/ foreclose the Security Deposit / recover from outstanding amount to the credit of the selected bidder towards the non- performance/non-compliance of the terms and conditions of the contract and/ or to recover the dues payable by the bidder from any, to appropriate towards damages (as mentioned in Point-1 and Point-2).

Bidder's Obligation on termination If the Contract is terminated on Non-Performance/ contract expiry then –

- a. The bidder shall handover all documents / executable / Bank's Data or any other relevant information to the Bank in timely manner and in proper format as per scope of this RFP and shall also support the orderly transition to another vendor or to the Bank.
- b. During the transition, the bidder shall also support the Bank on technical queries/support on process implementation or in case of software provision for future upgrades
- c. During the transition, the bidder shall continue to provide services as per the terms of the Agreement until a 'New Service Provider' completely takes over the work. The bidder shall provide all reasonable assistance, knowledge transfer, data export, documentation, credentials, configurations and cooperation required for an orderly transfer to the Bank or a replacement provider, without service degradation or withholding of Bank Data. During the transition phase, the bidder shall render all reasonable assistance to the new Service Provider within such period prescribed by the Bank, at no extra cost to the Bank, for ensuring smooth switch over and continuity of services, provided where transition services are required by the Bank or New Service Provider beyond the term of this Agreement, reasons for which are not attributable to the bidder, payment shall be made to the bidder for such additional period on the same rates and payment terms as specified in this Agreement.
- d. If bidder is in breach of the obligations mentioned in the Point 1, 2 and 3, the bidder shall be liable for paying a penalty (as per the SLAs) on demand to the Bank, which may be settled from the payment of invoices or Bank Guarantee for the contracted period or by invocation of Bank Guarantee.

13.19 Consequences of Termination

In the event of termination of the Contract due to any cause whatsoever, [whether consequent to the stipulated term of the Contract or otherwise], the Bank shall be

entitled to impose any such obligations and conditions and issue any clarifications as may be necessary to ensure an efficient transition and effective business continuity of the Service(s) which the Bidder shall be obliged to comply with and take all available steps to minimize loss resulting from that termination/breach, and further allow the next successor Bidder to take over the obligations of the erstwhile Bidder in relation to the execution/continued execution of the scope of the Contract.

In the event that the termination of the Contract is due to the expiry of the term of the Contract, a decision not to grant any (further) extension by the Bank, the Bidder herein shall be obliged to provide all such assistance to the next successor Bidder or any other person as may be required and as The Bank may specify including training, where the successor(s) is a representative/personnel of The Bank to enable the successor to adequately provide the Service(s) hereunder, even where such assistance is required to be rendered for a reasonable period that may extend beyond the term/earlier termination hereof. Nothing herein shall restrict the right of The Bank to invoke the Performance Bank Guarantee and other guarantees, securities furnished, enforce the Deed of Indemnity and pursue such other rights and/or remedies that may be available to The Bank under law or otherwise. The termination hereof shall not affect any accrued right or liability of either Party nor affect the operation of the provisions of the Contract that are expressly or by implication intended to come into or continue in force on or after such termination.

13.20 Audit by Third Party

Bank, its internal and external auditors, RBI, CERT-In, the Data Protection Board of India and any other competent governmental, statutory or regulatory authority, and their authorised representatives, may inspect and audit the selected bidder and every sub-contractor or sub-processor in relation to the Services, Bank Data and compliance with the Contract. Access shall extend to relevant premises, personnel, systems, networks, logs, records, reports, policies, controls, business-continuity arrangements and supporting evidence. The bidder shall provide timely cooperation, copies and explanations, remediate findings within the period directed by the Bank or regulator, and ensure equivalent rights in every downstream contract. Bank will incur the cost of appointment of a third party for audit. the bidder shall bear its own cooperation and remediation costs and the reasonable cost of any repeat or special audit necessitated by a material breach, incident or failed remediation. These rights shall survive while the bidder or any sub-contractor retains Bank Data or continues transition services. The selected Bidder shall allow the Bank, its authorized personnel, its auditors (internal and external) and/or other statutory authorities, Statutory Authorities shall have unrestricted right to inspect and audit the operations and records directly related to the services. The Cost & Accounting Records will be out of scope for the purpose of audit conducted by the Bank. If the selected Bidder is outsourcing any portion of the above activity, it will be the responsibility of the Successful Bidder to ensure that the authorities/officials as mentioned above are allowed access to the places, systems, processes, records (except Cost & Accounting Records) etc. of the activity, for inspection and verification. The Successful Bidder shall keep complete and accurate records of all the operations

in connection with the activities, per prevalent best practices in the industry. All books, records (except Cost & Accounting Records) and information relevant to the services shall be preserved in isolation and be presented to the Bank or its designees for inspection as and when demanded. The Bidder is required to facilitate the same at no additional cost. The Successful Bidder should recognize the right of Reserve Bank of India (RBI) to cause an inspection to be made of the Successful Bidder / service provider/ system integrator and its books and accounts by one or more of its officers or employees or other designated person. Prior intimation shall be shared with the bidder, regarding the audit so as to notify the Bank any potential conflict of interest.

The Bank will ordinarily give reasonable prior notice of an audit during normal business hours. No prior notice shall be required for a regulatory inspection, suspected fraud or security incident, material breach, urgent risk to Bank Data or systems, or where notice may prejudice the audit. Any confidentiality undertaking requested from an auditor shall not restrict disclosure of findings to the Bank, its governing bodies, professional advisers or competent authorities. The bidder shall not assert confidentiality, intellectual-property rights or sub-contractor restrictions to prevent or delay a lawful audit or regulatory access.

APPENDIX

APPENDIX 1: Functional & Technical Compliance Sheet:

- Generic, speculative & theoretical points should be avoided in the responses.

Attached as a separate Excel file.

- Exceptions, disclaimers, limitations, conditional compliance submitted by bidder and OEMs in the bid shall not be taken on record and selected bidder & respective OEM must mandatorily provide such features, modules, add-ons, service etc. sought by the Bank in the RFP.
- Generic, speculative & theoretical points should be avoided in the responses and shall be considered null and void

Sr. No.	Requirement Description	Compliance (Y/N)	Detailed Response
1	Generate and serve notices meeting Section 5 of the DPDP Act, itemising personal data collected, purposes, rights and the route to the Data Protection Board of India.		
2	Notices shall be drafted in plain, non-legalistic language, with a readability standard agreed with the Bank.		
3	English plus all 22 languages of the Eighth Schedule to the Constitution, with per-language versioning and a translation workflow.		
4	Data principal shall be able to select and change the language in which notices are served, with the preference persisted.		
5	Structured review workflow with DPO sign-off, full version history, and the ability to reproduce the exact notice version served to any data principal on any past date.		
6	Notice delivery across web, mobile, branch, contact centre, SMS, email and physical forms, with delivery confirmation and evidence capture.		
7	Automatic identification of data principals requiring a fresh notice when purposes or processing materially change, with campaign management.		
8	Central searchable repository of all notice versions with effective-from and effective-to dates.		
9	Notice rendering API and embeddable widget consumable by web, mobile, applications, returning		

Sr. No.	Requirement Description	Compliance (Y/N)	Detailed Response
	the correct version and language for the data principal.		
10	Integration with the Bank's SMS, email and push gateways for notice dispatch, with delivery, bounce and read status written back as evidence.		
11	Purpose-specific, granular consent at the UCIC or Customer-ID level, with hierarchical consent structures and configurable templates.		
12	Consent templates configurable to DPDP, RBI, IRDAI and UIDAI requirements where the Bank distributes or cross-sells third-party products.		
13	Consent capture across digital, physical-subsequently-digitised and third-party-agency collected modes, with equal evidentiary standing.		
14	Withdrawal shall be as easy as grant, with real-time propagation to every integrated system and enforcement of downstream processing halt.		
15	Self-service preference centre allowing data principals to view, modify and withdraw consent and see live consent status.		
16	Data principals shall be able to check consent status on a real-time basis through any Bank channel.		
17	Verifiable parental or legal-guardian consent for children and for persons with disability, with age verification and guardian-identity checks as required under the DPDP Rules.		
18	Configurable age-gating logic that blocks processing of a child's data for prohibited purposes such as behavioural tracking and targeted advertising.		
19	Tamper-evident consent artefacts capturing timestamp, notice version, purpose, channel, exportable for audit and DPBI submission.		
20	Consent artefacts shall be immutable and admissible as evidence, aligned to MeitY's Electronic Consent Framework.		
21	A mechanism for internal systems to validate a data principal's current consent status before any processing occurs.		

Sr. No.	Requirement Description	Compliance (Y/N)	Detailed Response
22	Consent retention and expiry rules with automated renewal or re-consent campaigns, and alerts ahead of expiry.		
23	Multi-channel notification to the data principal on consent capture, modification, expiry and withdrawal.		
24	Ability to act as, or interoperate with, a registered Consent Manager under the DPDP Rules when the ecosystem goes live.		
25	Bulk consent capture, bulk notice issuance and bulk withdrawal handling for legacy and migrated customer sets.		
26	Analytics on consent rates, withdrawal rates, purpose-wise uptake and channel effectiveness.		
27	Consent grant, change, expiry and withdrawal published as events to the Bank's event bus or via webhooks, so downstream systems react without polling.		
28	Defined, Bank-approved fail-safe behaviour when the consent service is unreachable; the default shall never be to process without consent.		
29	Workflows where consent revocation for services take effect within defined timelines across all relevant systems?		
30	Automated workflow to remove/mask/anonymize consent-captured attributes from SSOT and derived stores (data marts/feature stores/analytics extracts) where legal/regulatory retention does not require keeping it		
31	WCAG 2.1 AA compliant, fully brandable banner supporting geo-fencing and category-based consent (Strictly Necessary, Functional, Analytical, Marketing).		
32	Strict prior blocking of all non-essential cookies, until affirmative consent.		
33	Automated periodic scan of all Bank websites to detect new or changed trackers, with alerting to the privacy team.		

Sr. No.	Requirement Description	Compliance (Y/N)	Detailed Response
34	Automatic categorisation of discovered cookies against a maintained cookie database		
35	Proof-of-consent log for every visitor, retained for the statutory period and exportable on demand.		
36	Persistent, easily accessible control allowing a visitor to change or withdraw cookie consent at any time.		
37	Banner deployable with no measurable impact on page performance.		
38	The solution should have ability to create a customized cookie banner for each scanned website		
39	The solution should have ability to configure "consent" to be? For example, "opt out of all" or "opt out of one or more", etc.		
40	The solution should have ability to support cookie policy versioning to ask users for re-consent		
41	The solution should have ability to remember the cookie choices stored in the browser once the user returns		
42	The solution should have ability to have a reporting dashboard and allow you to export compliance reports		
43	End-to-end automated handling of access, correction, completion, updation, erasure, nomination and grievance redressal requests.		
44	Request intake through web, mobile, branch, contact centre, email ..., all converging into a single queue.		
45	Configurable SLA clocks aligned to the statutory grievance timeline and the Bank's internal thresholds, with escalation, ageing and breach alerts.		
46	Pre-configured, statutorily compliant response templates for each right, with DPO-approved wording and version control.		

Sr. No.	Requirement Description	Compliance (Y/N)	Detailed Response
47	Capture, validation, update and revocation of nominees, enabling a nominee to exercise rights in accordance with the Act and the Bank's terms.		
48	Configurable handling of erasure requests where retention is mandated by law or by RBI, with a documented and communicated reason for refusal.		
49	Grievance workflow with escalation to the DPO and onward tracking of any DPBI complaint.		
50	Immutable audit trail documenting every stage of request handling, from intake to closure.		
51	On-demand CSV and PDF exports of request volumes, outcomes, SLA performance and supporting evidence, in DPBI-ready format.		
52	Ability to absorb a surge in requests without SLA degradation, including a bulk-request scenario		
53	Automated acknowledgement, status updates and closure communication to the data principal on their preferred channel.		
54	Solution to track receipt and closure dates for each DSR and respond within defined timelines with an auditable trail.		
55	The system should maintain tamper-proof logs of actions taken, responses shared, and processors contacted.		
56	The system should generate export-ready formats for reports and notifications to the Data Protection Board (DPB).		
57	The system should auto-send acknowledgments/notifications to data principals upon receipt of their request.		
58	The solution should have ability to offer an appeal option to data principals if the submitted report is not up to satisfaction by the data principal		
59	Automated discovery across RDBMS, Data warehouse and data lake sources, on-premise and cloud.		
60	Discovery across file shares, SharePoint on-premise and online, OneDrive, object storage, email archives and endpoints.		

Sr. No.	Requirement Description	Compliance (Y/N)	Detailed Response
61	Discovery across logs, JSON and XML stores, message queues and API payload repositories, OCR-based discovery within scanned documents and image files.		
62	Discovery options across endpoints, file shares, databases and supported cloud repositories.		
63	One-time comprehensive full scan before go-live, plus scheduled full and incremental scans		
64	Automatic discovery of newly added databases, schemas and tables on a scheduled basis, with alerting to the data owner.		
65	Automatic identification and multi-level classification of personal data including Aadhaar, PAN, account numbers, biometrics, and financial behaviour data.		
66	Bank-defined custom classifiers and classification hierarchies, configurable without OEM involvement.		
67	End-to-end personal data automated flow mapping across systems, processors.		
68	Encryption, masking and access revocation ... on discovered exposures.		
69	Scan results shall be stored as metadata and location references; the platform shall not create a secondary copy of the discovered personal data.		
70	Generate automated visual lineage diagrams to illustrate the flow of data.		
71	Capture and store metadata for each data element, including creation date, modification history/ versioning with notifications to Business owner/ DPO team		
72	The solution should have ability to perform sensitive data discovery supported in unstructured text		
73	The solution should have ability to support data mapping initiatives, including mapping and analyzing assets and processing activities		
74	The solution should have ability for central dashboard with sorting and filtering capabilities of discovered data/meta data		

Sr. No.	Requirement Description	Compliance (Y/N)	Detailed Response
75	Ability to identify duplicate/near duplicate files/documents		
76	Solution should be hosted within Indian geography considering data localization requirements from various regulatory bodies i.e. RBI, CERT-IN, DPDPA, NCIIPC etc		
77	The solution should have ability to identify obsolete files and documents based on defined criteria. For e.g. find all the HR documents which are older than 3 years OR find all the documents older than 5 years having PII & Sensitive data).		
78	Maintain a living RoPA covering purpose, legal basis, data categories, data principals....		
79	RoPA entries to auto-populate from discovery and lineage outputs rather than manual data entry.		
80	Periodic attestation workflow requiring the business owner to confirm or correct each RoPA entry, with reminders and overdue tracking.		
81	Versioned change history with delta reporting and an automatic trigger into DPIA or threat-model reassessment on material change.		
82	Every RoPA entry shall be linked to the applicable notice version, consent purpose, DPIA and threat model.		
83	Each RoPA entry shall identify the processors and sub-processors involved and the contract governing the transfer.		
84	Regulator-ready RoPA export in CSV and PDF, filtered by business unit, purpose or data category.		
85	Reporting on RoPA coverage against the Bank's approved application inventory, highlighting gaps.		
86	Configurable DPIA questionnaires and workflow covering initiation, review, approval and closure, with a real-time status dashboard.		
87	Structured scoring of likelihood, impact and harm to the data principal, with a severity matrix mapped to the Bank's risk taxonomy.		

Sr. No.	Requirement Description	Compliance (Y/N)	Detailed Response
88	Automatic DPIA triggering for AI and ML decisioning, digital lending, profiling, cross-border transfer and children's data processing.		
89	Pre-built DPIA templates for common banking use cases, tailorable by the Bank without OEM involvement.		
90	Configurable approval hierarchy up to the DPO and, where required,		
91	Scheduled re-assessment of completed DPIAs and automatic re-opening on material change.		
92	Central repository of completed DPIAs with attachments, decisions and approvals, searchable and exportable.		
93	Questionnaire, scoring and approval workflow configurable by the Bank's administrator without code change or OEM involvement.		
94	API to receive Privacy Threat Modelling export packs and attach them to the corresponding DPIA record automatically.		
95	Detection and intake of personal data breaches across on-premise, cloud..., with SIEM and DLP correlation.		
96	Manual breach reporting channel for employees, vendors and data principals, with anonymous reporting option.		
97	Guided triage assigning severity based on data categories, volume, sensitivity and likely harm to data principals.		
98	Structured containment, eradication and recovery workflow with task assignment and immutable timeline.		
99	Automated impact analysis identifying affected data principals, data categories and downstream systems from discovery and lineage data.		
100	Templated intimation to the Data Protection Board of India within the timelines prescribed by the DPDP Rules, with dispatch evidence retained.		
101	Individual notification to affected data principals in the prescribed form and language, across the Bank's channels, with delivery tracking.		

Sr. No.	Requirement Description	Compliance (Y/N)	Detailed Response
102	Intake and management of breaches originating at a processor or partner, with contractual notification clocks tracked.		
103	Breach outcomes shall feed back into threat models, DPIAs and control design, with the linkage recorded.		
104	Bulk notification dispatch to affected data principals with throttling, retry and delivery evidence, without overwhelming Bank gateways.		
105	Central register of all data processors, sub-processors, fintech partners and DSAs handling Bank personal data, with contract linkage.		
106	Privacy due-diligence questionnaire and risk scoring at processor onboarding, with approval gates.		
107	Automated periodic reassessment of processors against contractual privacy obligations, with evidence collection and scoring.		
108	Automatic flagging of missing privacy-by-contract provisions, data residency non-compliance and control gaps, routed to remediation with tracked closure.		
109	Visibility into sub-processors engaged by each processor, with notification obligations tracked.		
110	Register of all personal data shared with each third party, the purpose, the legal basis and the retention obligation.		
111	Third-party privacy risk dashboard showing inherent and residual risk, open findings and overdue remediation.		
112	External vendor portal allowing processors to respond to questionnaires and upload evidence directly, with access controls and expiry.		
113	Route requests from Data Principal Rights Management to processor (Manual and auto) if received any		
114	Create, assign Third party risk assessments to vendors and manage the lifecycle.		
115	The system should flag non-compliance with contractual clauses related to data breach, retention, deletion, etc.		

Sr. No.	Requirement Description	Compliance (Y/N)	Detailed Response
116	The system should monitor contract renewal dates and notify internal stakeholders for review or renegotiation.		
117	Customizable dashboard for the DPO, Executive.		
118	Bank-configurable reports for internal audit, statutory audit, RBI inspection and DPBI inquiry, with scheduled distribution.		
119	Self-service report builder allowing the Bank's team to create new reports without OEM or bidder effort.		
120	Every dashboard figure shall reconcile exactly to the underlying records; exported CSV and PDF shall match the on-screen view without discrepancy.		
121	Classify personal data by category and apply retention rules automatically, driven by purpose, legal basis and lifecycle stage.		
122	Automatic triggering of secure deletion, compliant archival or de-identification at end of life, with auditable evidence.		
123	A privacy threat library covering BFSI datasets, channels, common API patterns and integration archetypes, extensible by the Bank.		
124	Threat modelling shall analyse the full personal data lifecycle — ingress, storage, use, sharing, retention and deletion — identifying misuse, overexposure and control gaps at each stage.		
125	Applicable to core banking, internet and mobile banking, digital lending journeys, UPI and payment rails, fintech and partner APIs, and any application processing personal data.		
126	A BFSI-adapted threat modelling playbook containing standardised DFD conventions, modelling templates, documentation standards and a privacy threat catalogue for Indian banking.		
127	Stop processing for withdrawn consent purpose i.e. cease processing consent-dependent data for that purpose within a defined timelines (e.g., profiling/ personalization...)		
128	Automated Workflows where consent revocation/ modification for services take effect within defined timelines.		

Sr. No.	Requirement Description	Compliance (Y/N)	Detailed Response
129	Stop processing for withdrawn consent purpose i.e. suppresses the customer from outbound campaigns across SMS, WhatsApp, email, app push, and outbound calls		
130	The proposed solution shall provide transparent data-centric encryption without requiring modification to application source code.		
131	The proposed solution shall not require changes to database schema, table structure, or existing business workflows.		
132	The solution shall support encryption of structured sensitive data including Aadhaar, PAN, mobile number, email ID, financial records, and other Personally Identifiable Information (PII).		
133	The solution shall support policy-based decryption based on user identity, application identity, role, device, location, or purpose of access.		
134	Unauthorized users shall view masked, anonymized, tokenized, or encrypted values based on defined security policies.		
135	The solution shall support tokenization and anonymization capabilities..		
136	The solution shall support automatic encryption of newly inserted or modified records..		
137	The solution shall support integration with enterprise IAM, PAM, SIEM, SOC, and governance systems.		
138	The solution shall support high availability and failover deployment architecture.		
139	The solution shall support AES-256 and Quantum Proof Encryption algorithms.		
140	Solution shall support Data Masking (DDM) for real-time masking of sensitive information		
141	Data masking must not degrade Finacle or core banking transaction speeds		
142	Solution shall support masking of PII, PCI, financial, DPDP data categories, and the data as and when required by the Bank.		
143	Solution shall support masking for development, testing, analytics, and training environments.		

Sr. No.	Requirement Description	Compliance (Y/N)	Detailed Response
144	Solution shall support referential integrity preservation after masking		
145	Solution shall support compliance initiatives related to DPDPA		
146	The system should allow for periodic re-assessment of DPIAs based on changes in processing or legislation.		
147	The solution should provide built-in Dictionaries		
148	The solution should have proximity be configured for higher detection efficacy		
149	The solution should have ability to support configurable parameters in Universal Consent API		
150	The system should be able to issue downloadable consent receipts to data principals with purpose and timestamp references		

APPENDIX 2 : Commercial Bill of Materials

Table 1 - Volumetric

- The Bidder must specify details of Hardware required for successful implementation of the offered Solution based on below Volumetric

Sr.	Solution	Volumetric
1	DPDP Compliance Suite	HA deployment (active/passive) at DC and DR, DR at full DC capacity
2		1.5 crore + customers in total; 85 lakh+ active customers to be used for sizing
3		Up to 250+ business applications to be integrated with DPDP suite
4		Up to 20,000 endpoints for data discovery and classification
5		Bank-wide discovery and scanning of structured and unstructured data sources
6		ROPA and DPIA records for up to 250+ applications and business processes
7		At least 30% headroom over these numbers at no additional licence cost

Table 2 - Infrastructure sizing

Sr.	Parameter	DC	DR	UAT	Bidder's remarks
1	Virtual servers (Windows / RHEL / Ubuntu) on VMware VCF				
2	vCPU per node (state clock speed and core count)				
3	RAM per node				
4	Primary storage per node				
5	Oracle DB licence (ULA)				
6	AVI load balancer				
7	Backup infrastructure				
8	SAN NVMe storage, S3 storage				

Sr.	Particulars	Quantity	Location	Make and version	OEM / OSD	Complies (Yes/No)
1	Data protection suite for DPDP compliance, as per the technical specification and scope of work					
2	Privacy Enhancing Technologies (PET)					
3	Privacy Threat Modelling (PTM)					
4	Others					

(Add as many rows as required)

*** If proposed solution requires any other OS, DB license or Hardware apart from the above specified, then bidder has to provide those details separately by adding as many rows wherever required in the above table and absorb the cost within the TCO.**

Vendor must provide the necessary GPU/ hardware requirements for AI models or any other in scope DPDP solution/ Software modules if used. The same must be incorporated in TCO (including supply, install, configure, integrate GPU and related hardware peripherals if needed). The solution suite and all AI components must be deployed strictly on the bank's physical, on-premises Infra with isolation and no external network connectivity. No outbound telemetry, metadata, prompt tokens, or system diagnostic metrics containing Company data shall leave the Bank's network or be transmitted to any public, multi-tenant, or overseas cloud environment under any circumstances.

The Bidder is expected to:

- Size the infrastructure (Hardware, Operating System, Database and other related software) for the solution based on the volume and the growth and propose the same as part of their technical bid submission. Bank may use existing IT infrastructure or procure separately the required infrastructure based on the sizing proposed by the vendor. However, the complete setup of Solution and any other hardware apart from the above specification at DC, DR, UAT & Pre-prod shall be part of the scope of the vendor.
- The resource including CPU utilization of any server/ appliance should not go beyond 70%. If the same crosses the threshold of 70% five times in a day or 10 times in a week, bidder should fine tune the application to ensure the utilization within the aforesaid threshold without any additional cost to the bank.
- **RHEL/Windows OS licenses and Oracle Database licenses required, if any, will be provided by the bank.**

- **If proposed solution requires any other OS, DB license or Hardware apart from the above specified, then bidder has to provide those details separately and absorb the cost within the TCO.**
- Exceptions, disclaimers, limitations, conditional compliance submitted by bidder and / or OEMs in the bid shall not be taken on record and selected bidder & respective OEM must mandatorily provide such features, modules, add-ons, service etc. sought by the bank in the RFP.
- Generic, speculative & theoretical points should be avoided in the responses and shall be considered null and void
- The Bidder to ensure that the supplied GPU hardware and peripherals are compatible with the Bank's existing Infrastructure stack in the respective DC & DR
- Upon physical delivery and successful deployment, absolute title, legal ownership, and unencumbered proprietary rights of the supplied GPU hardware and all associated peripherals shall automatically transfer to the Bank
- The Bank shall retain uninhibited rights to reallocate, repurpose, upgrade, or utilize the GPU hardware for any future use within the scope of this project, without requiring consent from or payment of any additional royalty/license fee to the Vendor. OEM back-to-back enterprise warranties (minimum [3] years) and hardware support contracts must be registered directly in the name of the Bank.

Table A1: Enterprise-wide Perpetual Software licence and support cost, DC

Sr.	Module / item	Cost model and unit basis	Licence cost	Year 1 (₹) year	Year 2 (₹) ATS	Year 3 (₹) ATS	Total 3 years (₹)
1	Notice & Consent Management	Enterprise-wide, bank-wide use					
2	Cookie Management	Enterprise-wide, bank-wide use					
3	Data Principal Rights Management	Enterprise-wide, bank-wide use					
4	Third Party Risk Management	Enterprise-wide, bank-wide use					
5	Personal Data Discovery and Data Security Posture Management	Enterprise-wide, bank-wide use					
6	Records of Processing Activities / Data Protection Impact Assessment	Enterprise-wide, bank-wide use					
7	Data Breach and Incident Management	Enterprise-wide, bank-wide use					
8	Privacy Enhancing Technologies	Enterprise-wide, bank-wide use					
9	Privacy Threat Modelling	Enterprise-wide, bank-wide use					
10	Privacy Training Awareness	Enterprise-wide, bank-wide use					
11	Dashboard and Reporting, Audit Logs	Enterprise-wide, bank-wide use					

Sr.	Module / item	Cost model and unit basis	Licence cost	Year 1 (₹) year	Year 2 (₹) ATS	Year 3 (₹) ATS	Total 3 years (₹)
12	Any Other Requirement like solution/Graphical Processing Unit (GPU)/etc (specify)	Enterprise-wide, bank-wide use					
	Total licence and support cost (A1)	DC					

(Add as many rows as required)

Table A2: Enterprise-wide Perpetual Software licence and support cost, DR

Sr.	Module / item	Cost model and unit basis	License cost	Year 1 (₹) year	Year 2 (₹) ATS	Year 3 (₹) ATS	Total 3 years (₹)
1	Notice & Consent Management	Enterprise-wide, bank-wide use					
2	Cookie Management	Enterprise-wide, bank-wide use					
3	Data Principal Rights Management	Enterprise-wide, bank-wide use					
4	Third Party Risk Management	Enterprise-wide, bank-wide use					
5	Personal Data Discovery and Data Security Posture Management	Enterprise-wide, bank-wide use					

Sr.	Module / item	Cost model and unit basis	License cost	Year 1 (₹) year	Year 2 (₹) ATS	Year 3 (₹) ATS	Total 3 years (₹)
6	Records of Processing Activities / Data Protection Impact Assessment	Enterprise-wide, bank-wide use					
7	Data Breach and Incident Management	Enterprise-wide, bank-wide use					
8	Privacy Enhancing Technologies	Enterprise-wide, bank-wide use					
9	Privacy Threat Modelling	Enterprise-wide, bank-wide use					
10	Privacy Training Awareness	Enterprise-wide, bank-wide use					
11	Dashboard and Reporting, Audit Logs	Enterprise-wide, bank-wide use					
12	Any Other Requirement like solution/Graphical Processing Unit (GPU)/etc (specify)	Enterprise-wide, bank-wide use					
	Total licence and support cost (A2)	DR					

(Add as many rows as required)

Table A3: Enterprise-wide Perpetual Software licence and support cost, UAT and Pre-prod

Sr.	Module / item	Cost model and unit basis	Licence cost	Year 1 (₹) year	Year 2 (₹) ATS	Year 3 (₹) ATS	Total 3 years (₹)
1	Notice & Consent Management	Enterprise-wide, bank-wide use					
2	Cookie Management	Enterprise-wide, bank-wide use					
3	Data Principal Rights Management	Enterprise-wide, bank-wide use					
4	Third Party Risk Management	Enterprise-wide, bank-wide use					
5	Personal Data Discovery and Data Security Posture Management	Enterprise-wide, bank-wide use					
6	Records of Processing Activities / Data Protection Impact Assessment	Enterprise-wide, bank-wide use					
7	Data Breach and Incident Management	Enterprise-wide, bank-wide use					
8	Privacy Enhancing Technologies	Enterprise-wide, bank-wide use					
9	Privacy Threat Modelling	Enterprise-wide, bank-wide use					
10	Privacy Training Awareness	Enterprise-wide, bank-wide use					
11	Dashboard and Reporting, Audit Logs	Enterprise-wide, bank-wide use					

Sr.	Module / item	Cost model and unit basis	Licence cost	Year 1 (₹) year	Year 2 (₹) ATS	Year 3 (₹) ATS	Total 3 years (₹)
12	Any Other Requirement like solution/Graphical Processing Unit (GPU)/etc (specify)	Enterprise-wide, bank-wide use					
	Total licence and support cost (A3)	UAT					

(Add as many rows as required)

Table B — Implementation and integration cost

Sr.	Item	Implementation cost (₹)	Year 1 (₹)	Year 2 (₹)	Year 3 (₹)	Total (₹)
1	Installation and implementation at DC		<i>Not applicable</i>	<i>Not applicable</i>	<i>Not applicable</i>	-
2	Installation and implementation at DR		<i>Not applicable</i>	<i>Not applicable</i>	<i>Not applicable</i>	-
3	Installation and implementation of the UAT set-up		<i>Not applicable</i>	<i>Not applicable</i>	<i>Not applicable</i>	-
4	Integration of applications (up to 250) including all upstream and downstream applications & touchpoints at enterprise level		<i>Not applicable</i>	<i>Not applicable</i>	<i>Not applicable</i>	-
5	Total implementation cost (B)		<i>Not applicable</i>	<i>Not applicable</i>	<i>Not applicable</i>	-
	Rate Card for each application integrated beyond 250					

Table C — Consultancy services cost

- Three consultancy resources onsite in year 1; one resource in each of years 2 and 3.

Sr.	Consultancy resource	Rate per month (₹)	Year 1 (₹)	Year 2 (₹)	Year 3 (₹)	Total (₹)
1	Lead DPDP consultant					
2	Privacy consultant (legal / compliance)					
3	Privacy analyst					
	Total consultancy cost (C)					
Sr.	RATE CARD per Additional Resource	Rate per month				
1	Privacy consultant (legal / compliance)					
2	Privacy analyst					

Table D — Facility Management cost

Sr.	Resource	Count	Rate per month (₹)	Year 1 (₹)	Year 2 (₹)	Year 3 (₹)	Total (₹)
1	Project Manager	1					
2	SME / Legal	1					
3	L1 onsite support engineer	4					
4	L2 onsite support engineer	2					
	Total Facility Management cost (D)	8					
Sr.	RATE CARD per Additional Resource	Rate per month					
1	L1 onsite support engineer						
2	L2 onsite support engineer						

Table E —Total Cost of Ownership — 3-year contract

- Each figure comes from its own tables. All figures are exclusive of taxes.

Sr.	Cost head	Amount (₹)
1	Enterprise-wide Perpetual Licence and support — DC (A1)	
2	Enterprise-wide Perpetual Licence and support — DR (A2)	
3	Enterprise-wide Perpetual Licence and support — UAT (A3)	
4	Implementation and integration cost (B)	
5	Consultancy services cost (C)	
6	Facility Management cost (D)	
	TOTAL COST OF OWNERSHIP	
	Total in words	

ANNEXURES

Annexure 1: Submission Checklist (on bidder's letterhead)

S.No.	Particulars	Submitted (Yes/No)	Page No
1.	Tender Covering letter		
2.	Bidder's Information		
3.	Bid Security Declaration		
4.	Pre-Qualification Criteria		
5.	Acceptance/Compliance Certificate		
6.	Manufacturer's Authorization form		
7.	Escalation matrix		
8.	Litigation Certificate		
9.	Non- Blacklisting undertaking		
10.	Undertaking of Authenticity		
11.	Non-Disclosure agreement		
12.	Commercial proposal submission checklist		
13.	Bank guarantee Format for Earnest Money Deposit		
14.	Performance guarantee		
15.	Pre-contract integrity pact		
16.	Compliance with Scope of Work & SBOM		
17.	S-BOM & C-BOM Details of all the proposed Tool/ solutions		
18.	Minimum Local Content Certification		
19.	Proposed Resources CV		
20.	Client Reference		
21.	Hardware Sizing, Infrastructure as per Appendix 2		
22.	Functional and Technical Specifications response sheet		
23.	Undertaking for Being the OEM/OSD of offered Product		
24.	Signed Copy of RFP and addendum/ Corrigendum (If any)		
25.	Masked appendix Commercial Bid		

Note:

- All pages of the bid documents must be sealed & signed in full by authorized person.
- All pages of the bid documents should be numbered in serial order i.e. 1, 2, 3....
- Bank may ask for any other document on its discretion.

Date ,Signature & Seal of the Bidder

Annexure 2: Bidder's Information

Bidder's Information

(Should be submitted on Company's letter head with company seal and signature of the authorized person)

Reg: Request for Proposal (RFP) for Procurement of DPDP Suite and selection of System Integrator (SI) cum Consultant services for Supply, Installation, Integration, Implementation and Management of Digital Personal Data Protection Solution for a period of 3 Years

Ref: RFP No. _____ dated _____

Sr No	Particulars	Details
1.	Name of the Company Address for Correspondence: Registered Office: Corporate Office:	
2.	Constitution (Proprietary/Partnership/Private Ltd./Public Ltd./ LLP/ Others)	
3.	Registration No. and date of establishment	
4.	Website Address	
5.	Email Address	
6.	Number of Years in the Business	
7.	Detail of Earnest Money Deposited.	
8.	If any exemption is required with respect to EMD or Start-up.	
9.	Income Tax PAN GSTN ID <u>Beneficiary Bank Details</u> Beneficiary Name Beneficiary Account Number Type of Account (OD/OCC etc.) IFSC Name of the Bank and Branch address	
10.	Single Point of contact for this RFP Name: Designation: Mobile No.: Landline No.: Email-ID	

Sr No	Particulars	Details
	(any changes in the above should be informed in advance to Bank)	
11.	Name of Person Authorized to sign Designation. Mobile No. Email Address	

Wherever applicable submit documentary evidence to facilitate verification.

DECLARATION:

I/We hereby declare that the terms and conditions of the tender stated herein and as may be modified/mutually agreed upon are acceptable and binding to me/us. We understand and agree and undertake that: -

- 1) The Bank is not bound to accept the lowest bid or may reject all or any bid at any stage at its sole discretion without assigning any reason, therefore.
- 2) If our Bid for the above job is accepted, we undertake to enter into and execute at our cost, when called upon by the Bank to do so, a contract in the prescribed form. Unless and until a formal contract is prepared and executed, this bid together with your written acceptance thereof shall constitute a binding contract between us.
- 3) We have read and understood all the terms and conditions and contents of the RFP and also undertake that our bid conforms to all the terms and conditions and does not contain any deviation and misrepresentation. We understand that the Bank reserves the right to reject our bid on account of any misrepresentation/deviations contained in the bid.
- 4) Bank may accept or entrust the entire work to one Bidder or divide the work to more than one bidder without assigning any reason or giving any explanation whatsoever and the Bank's decision in this regard shall be final and binding on us.
- 5) I/ We do not have any conflict of interest as mentioned in the RFP document.
- 6) I/We submit this application under and in accordance with the terms of the RFP document and agree and undertake to abide by all the terms and conditions of the RFP document.
- 7) The Prices submitted by us have been arrived at without agreement with any other Bidder of this RFP for the purpose of restricting competition.
- 8) The prices submitted by us have not been disclosed and will not be disclosed to any other Bidder responding to this RFP.
- 9) We have not induced or attempted to induce any other Bidder to submit or not to submit a Bid for restricting competition.
- 10) We have quoted for all the services/items mentioned in this RFP in our price Bid.
- 11) The rate quoted in the price Bids are as per the RFP and subsequent pre-Bid clarifications/ modifications/ revisions furnished by the Bank, without any exception.
- 12) We agree to the splitting of order in the proportion as stated in the RFP at the discretion of Bank.

- 13) We certify that while submitting our Bid document, we have not made any changes in the contents of the RFP document, read with its amendments/clarifications provided by the Bank.
- 14) If our bid is accepted, we are to be jointly and severally responsible for the due performance of the contract.
- 15) We ensured that salary payments to resources deployed for Bank's Project is done through Transfer mode from bidder's Bank a/c directly to credit into their specific salary accounts only. No cash payments are to be made to provide remuneration for services provided to the Bank on behalf of the selected bidder.
- 16) Bidder means the vendor(s) who is decided and declared so after examination of commercial bids.
- 17) We ensure that the entire data relating to payment systems operated by them will be stored in a system only in India. This data should include the full end-to-end transaction details / information collected / carried / processed as part of the message / payment instruction.
- 18) We confirm that Payment of statutory dues like PF, ESIC etc. are being made on time to the employees.

Dated this ____ day of _____, 2026

Bidder's Authorized Signatory

Designation

Bidder's name

Company Name and Seal

Annexure 3: Tender Covering Letter

(Should be submitted on Company's letter head)

To

Deputy General Manager (Data Protection Office)

Punjab and Sind Bank

Second Floor, DPO Department, Corporate Office, NBCC Building Block 3,
East Kidwai Nagar, New Delhi – 110023

Dear Sir,

Sub: Reg: Request for Proposal (RFP) for Procurement of DPDP Suite and selection of System Integrator (SI) cum Consultant services for Supply, Installation, Integration, Implementation and Management of Digital Personal Data Protection Solution for a period of 3 Years

Ref No. _____ dated _____

With reference to the above RFP, having examined and understood the instructions including all annexure, terms and conditions forming part of the Bid, we hereby enclose our offer for System Integrator cum Consultant and DPDP Solution Suite in the RFP document forming Technical Bid as well as Commercial Bid being parts of the above referred Bid. I am authorized to sign the documents in this regard and the copy of authorization letter/ POA / Board resolution is attached herewith.

We agree to abide by and fulfil all the terms and conditions of the tender and in default thereof, to forfeit and pay to you or your successors, or authorized nominees such sums of money as are stipulated in the conditions contained in tender together with the return acceptance of the contract.

We confirm that we have noted the contents of the RFP and have ensured that there is no deviation in filing our response to the RFP and that the Bank will have the right to disqualify us in case of any such deviations.

Until a formal contract is executed, this tender offer, together with the Bank's written acceptance thereof and Bank's notification of award, shall constitute a binding contract between us. We understand that The Bank is not bound to accept the lowest or any offer the Bank may receive. We also certify that we have not been blacklisted by any PSU Bank/IBA/RBI at the time of Bid submission.

All the details mentioned by us are true and correct and if the Bank observes any misrepresentation of facts on any matter at any stage, Bank has the absolute right to reject the proposal and disqualify us from the selection process. The Bank reserves the right to verify /evaluate the claims made by the Bidder independently.

Dated this ____ day of _____, 2026

Authorized Signatory

Designation

Bidder's name

(Name of Address Authorized Signatory)

Company Name and Seal

Annexure 4: Bid Security Declaration

Bid Security Declaration

(To be stamped in accordance with stamp act)

(Should be submitted by eligible MSEs/Startups on Company's letter head with company seal and signature of the authorized person)

Date:

To

Deputy General Manager (Data Protection Office)

Punjab and Sind Bank

Second Floor, DPO Department, Corporate Office, NBCC Building Block 3,
East Kidwai Nagar, New Delhi – 110023

Dear Sir,

We, the undersigned, declare that We, M/s..... (herein referred to as bidder) understand that, according to Bid clause 1.3 may be supported with a Bid Security Declaration, bidder render the declaration that:-

Bank may proceed against us for recovery of actual direct losses as per the remedy available under an applicable law (maximum up to Rs...../-) and In case of Execution of Bid Security Declaration, we, M/s.....may be suspend for three (3) years from being eligible to submit our bids for any contracts with the Bank if we, M/s..... are in breach of our obligation(s) under the bid conditions, in case we, M/s.....:-

- Fails to honor submitted bid; and/or
- If the bidder withdraws the bid during the period of bid validity (180 days from the date of opening of bid).
- If the bidder makes any statement or encloses any form which turns out to be false, incorrect and / or misleading at any time prior to signing of contract and/or conceals or suppresses material information; and / or
- The selected bidder withdraws his tender before furnishing the unconditional and irrevocable Performance Bank Guarantee.
- The bidder violates any of the provisions of the terms and conditions of this tender specification.
- In case of the successful bidder, if the bidder fails:
 - To sign the contract in the form and manner to the satisfaction of Punjab & Sind Bank
 - To furnish Performance Bank Guarantee in the form and manner to the satisfaction of Punjab & Sind Bank either at the time of or before the execution of Agreement.
 - Bank may proceed against the selected bidder in the event of any evasion, avoidance, refusal or delay on the part of bidder to sign and

execute the Purchase Order / Service Level Agreements or any other documents, as may be required by the Bank, if the bid is accepted.

We, M/s.....understand that this declaration shall expire if we are not the successful bidder and on receipt of purchaser's notification of the award to another bidder; or forty-five days after the validity of the bid; whichever is later.

Dated this ____ day of _____, 2026

Authorized Signatory

Designation

Bidder's name

(Name of Address Authorized Signatory) Company Name and Seal

Annexure 5: Pre-Qualification Criteria

Ref: RFP No._____ dated_____

We have carefully gone through the contents of the above-referred RFP along with replies to pre-bid queries & amendment, if any, and furnish the following information relating to Pre-Qualification Criteria.

Sr.	Eligibility Criteria	Supporting Documents be submitted	Bidder Response
1			

- The Bidder/OEM shall comply with all applicable CVC guidelines, the General Financial Rules, 2017 and Department of Expenditure instructions, as amended from time to time, including CVC guideline 3(a, b) circular no. 03/01/12, GFR Rule 16(a) of 2005 and OM of DOE dated 25/07/2016. For the same item or product, either the Principal/OEM may bid directly or its duly authorised Indian agent may bid on its behalf; both shall not bid simultaneously. An agent shall not submit bids for more than one Principal/OEM for the same item or product in this tender.
- If an agent submits bid on behalf of the principal/OEM, the same agent shall not submit a bid on behalf of another principal/OEM in the same tender for the same item/product.

Date

Signature with seal

Name:

Designation:

Annexure 6: Acceptance/Compliance Certificate

ACCEPTANCE/ COMPLIANCE CERTIFICATE

Ref: RFP No. _____ dated _____

All Terms and Conditions including scope of work

We hereby undertake and agree to abide by all the terms and conditions, scope of work & other terms stipulated by the Bank in this RFP including all addendum, corrigendum, clarification issued by Bank etc.

Punjab & Sind Bank is not bound by any other extraneous matters, assumptions, or deviations, even if mentioned by us either in our proposal or any subsequent deviations sought by us, whether orally or in writing, and the Bank's decision not to accept such extraneous conditions, assumptions, and deviations will be final and binding on us.

Any assumptions, deviation or exclusions may result in the disqualification of our bids.

We also understand that the Bank may not consider our assumptions, deviations or exclusions quoted by us anywhere in the proposal during the evaluation or during the contract period and we shall be liable make necessary arrangements at no additional cost to the Bank in order to meet the requirements stated in the RFP including all addendum, corrigendum, clarification issued by Bank etc.

Signature:

Seal of company

Annexure 7: Manufacturer's Authorization Form (MAF)

MANUFACTURER'S AUTHORIZATION FORM

RFP No:

(Letter to be submitted by the OEM's letter head)

To

Deputy General Manager (Data Protection Office)

Punjab and Sind Bank

Second Floor, DPO Department, Corporate Office, NBCC Building Block 3,
East Kidwai Nagar, New Delhi – 110023

Dear Sir,

Sub: Reg: Request for Proposal (RFP) for Procurement of DPDP Suite and selection of System Integrator (SI) cum Consultant services for Supply, Installation, Integration, Implementation and Management of Digital Personal Data Protection Solution for a period of 3 Years

We, who are established and reputable manufacturers / producers of _____ having factories / development facilities at _____ (address of factory / facility) do hereby authorize M/s _____ (Name and address of Authorized Business Partner (ABP)) to submit a Bid and sign the contract with you against the above RFP.

1. We hereby extend our full ATS/AMC/Warranty support for the Products and services offered by the above _____ against the above RFP.
2. We also undertake to provide any or all of the following materials, notifications, and information pertaining to the Products supplied by the _____:
 - a. Such Products as the Bank may opt to purchase from the _____, provided that this option shall not relieve the ABP of any ATS/AMC Support /Warranty obligations under the RFP; and
 - b. In the event of termination of production of such Products:
3. Advance notification to the Bank of the pending termination, in sufficient time to permit the Bank to procure needed requirements; and following such termination, furnishing at no cost to the Bank operations manuals, standards and specifications of the Products, if requested.

4. We duly authorize the said _____ to provide on our behalf in fulfilling all installations, technical support and maintenance obligations required by the contract.
5. We hereby certify that we have read the clauses contained in O.M. No. 6/18/2019-PPD, dated 23.07.2020 order (Public Procurement No. 1), order (Public Procurement No. 2) dated 23.07.2020 and order (Public Procurement No. 3) dated 24.07.2020 regarding restrictions on procurement from a bidder of a country which shares a land border with India. We further certify that we are not from such a country or if from a country, have been registered with competent authority. We certify that we fulfil all the requirements in this regard and our ABP is eligible to participate in the above RFP.
6. We hereby extend our full guarantee and warranty as per terms and conditions of the Bid and the contract for the equipment, solution, and services offered against this invitation for Bid offer by the above firm. We undertake to provide back-to-back support for spare and skill to the bidder for subsequent transmission of the same to the Bank. We also undertake to provide support services during warranty as well as AMC/ATS period if the above bidder authorized by us fails to perform in terms of the RFP.

Place:

Name:

Date:

Phone No.:

Fax:

E-mail:

Annexure 8: Escalation Matrix

Escalation Matrix

(Should be submitted on Company's letter head with company seal and signature of the authorized person)

Ref: RFP No. _____ dated _____.

Name of the Company/Firm:

Service-Related Issues

Sr. No.	Name	Designation	Full Office Address	Phone No.	Mobile No.	Email address
1.		First Level Contact (Senior by designation to the project Director)				
2.		Second level contact (If response not received in 4 Hours)				
3.		Regional/Zonal Head (If response not received in 24 Hours)				
4.		Country Head (If response not received in 48 Hours)				

Any change in designation, substitution will be informed to Bank immediately.

Date

Signature with seal

Name:

Designation:

Annexure 9: Litigation Certificate

Litigation Certificate

Reg: Request for Proposal (RFP) for Procurement of DPDP Suite and selection of System Integrator (SI) cum Consultant services for Supply, Installation, Integration, Implementation and Management of Digital Personal Data Protection Solution for a period of 3 Years

To be provided by Statutory Auditor/Chartered Accountant

This is to certify that M/s _____, a company incorporated under the companies act, 1956 with its headquarters at, _____ is not involved in any litigation which threatens solvency of the company.

Date: _____

Place: _____

Signature of CA/Statutory Auditor

Name of CA/Statutory Auditor:

Designation:

Email ID:

Mobile No:

Telephone No.:

Seal of Company:

Annexure 10: Non-blacklisting undertaking

Undertaking for non-blacklisting

To
Deputy General Manager (Data Protection Office)
Punjab and Sind Bank
Second Floor, DPO Department, Corporate Office, NBCC Building Block 3,
East Kidwai Nagar, New Delhi – 110023

Dear Sir,

Reg: Request for Proposal (RFP) for Procurement of DPDP Suite and selection of System Integrator (SI) cum Consultant services for Supply, Installation, Integration, Implementation and Management of Digital Personal Data Protection Solution for a period of 3 Years

We M/s _____, a company incorporated under the companies act, 1956 with its headquarters at, _____ do hereby confirm that we have not been blacklisted/ debarred by the Government / Government agency / Banks / Financial Institutions in India during last 3 years.

This declaration has been submitted and limited to, in response to the tender reference mentioned in this document

Thanking You,

Yours faithfully,

Date: _____

Place: _____

Signature of Authorized Signatory

Name of Signatory:

Designation:

Email ID:

Mobile No:

Telephone No.:

Seal of Company:

Annexure 11: Undertaking of Authenticity (on bidder's letterhead)

To

Deputy General Manager (Data Protection Office)

Punjab and Sind Bank

Second Floor, DPO Department, Corporate Office, NBCC Building Block 3,
East Kidwai Nagar, New Delhi – 110023

Sub: Undertaking of Authenticity for supplied Product(s)

Ref: RFP No. <> Dated dd/mm/yyyy

With reference to the Product being quoted to you vide our Bid No: _____ dated _____, we hereby undertake that all the components /parts /assembly / software etc. used in the Product to be supplied shall be original new components / parts / assembly / software only, from respective Original Equipment Manufacturers (OEMs) of the Products and that no refurbished / duplicate / second hand components /parts/ assembly / software shall be supplied or shall be used or no malicious code are built-in in the Product being supplied.

1. We also undertake that in respect of licensed operating systems and other software utilities to be supplied, the same will be sourced from authorized sources and supplied with Authorized License Certificate (i.e. Product keys on Certification of Authenticity in case of Microsoft Windows Operating System).
2. Should you require; we hereby undertake to produce the certificate from our OEM supplier in support of above undertaking at the time of delivery/installation. It will be our responsibility to produce such letters from our OEM supplier's at the time of delivery or within a reasonable time.
3. In case of default and/or the Bank finds that the above conditions are not complied with, we agree to take back the Product(s) supplied and return the money paid by you, in full within seven days of intimation of the same by the Bank, without demur or any reference to a third party and without prejudice to any remedies the Bank may deem fit.
4. We also take full responsibility of both Product(s) & Service(s) as per the content of the RFP even if there is any defect by our authorized Service Centre / Reseller / SI etc.

Dated this day of 2026

(Signature)

(Name)

(In the capacity of)

Duly authorised to sign Bid for and on behalf of _____

Annexure 12: Non-Disclosure Agreement

NON-DISCLOSURE AGREEMENT

All bidders must sign the Non-Disclosure Agreement (NDA) while submitting the response to the Request for proposal (RFP). Bidders must comply with all clauses mentioned in the NDA. No changes to the NDA are allowed.

NDA format is provided below.

(To be stamped in accordance with stamp act)

Strictly Private and Confidential

This Non-Disclosure Agreement made and entered into at..... This day.....of.....20.....BY AND BETWEEN , a company incorporated under the Companies Act, 1956 having its registered office at (Hereinafter referred to as the Bidder which expression unless repugnant to the context or meaning thereof be deemed to include its permitted successors) of the ONE PART;

AND

Punjab and Sind Bank, a body corporate, established under the Banking Companies (Acquisition and Transfer of Undertakings) Act 1980 and having its (hereinafter referred to as "Bank" which expression shall unless it be repugnant to the subject, meaning or context thereof, be deemed to mean and include its successors and assigns) of the OTHER PART.

The Bidder and Punjab and Sind Bank are hereinafter collectively referred to as "the Parties" and individually as "the Party".

WHEREAS:

- 1) Punjab & Sind Bank is engaged in the business of providing financial services to its customers and intends to engage service provider _____
- 2) In the course of such an assignment, it is anticipated that Punjab & Sind Bank or any of its officers, employees, officials, representatives or agents may disclose, or deliver, to the Bidder some Confidential Information (as hereinafter defined), to enable the Bidder to carry out the aforesaid Implementation assignment (hereinafter referred to as " the Purpose").
- 3) The Bidder is aware and confirms that all information, data and other documents made available in the RFP/Bid Documents/Agreement /Contract or in connection with the Services rendered by the Bidder are confidential information and are privileged and strictly confidential and or proprietary of Punjab and Sind Bank. The Bidder undertakes to safeguard and protect such confidential information as may be received from Punjab and Sind Bank.

NOW, THEREFORE THIS AGREEMENT WITNESSED THAT in consideration of the above premises and the Punjab and Sind Bank granting the Bidder and or his agents,

representatives to have specific access to Punjab & Sind Bank property / information and other data it is hereby agreed by and between the parties hereto as follows:

4) Confidential Information:

- i) "Confidential Information" means all information disclosed/furnished by Punjab & Sind Bank to the Bidder whether orally, in writing or in electronic, magnetic or other form for the limited purpose of enabling the Bidder to carry out the proposed Implementation assignment, and shall mean and include data, documents and information or any copy, abstract, extract, sample, note or module thereof, explicitly designated as "Confidential"; Provided the oral information is set forth in writing and marked "Confidential" within seven (7) days of such oral disclosure.
- ii) Notwithstanding the foregoing definition and any marking requirement, "Confidential Information" includes all information disclosed or made available by Punjab & Sind Bank to the Bidder, before or after execution of this Agreement, in oral, written, visual, electronic, magnetic or any other form, for or in connection with the Purpose. It includes Bank Data, personal data, customer information, business and financial information, security information, credentials, configurations, vulnerabilities, audit material, documents, extracts, analyses and materials derived from such information, whether or not marked or identified as confidential. Oral information shall be protected if its nature or the circumstances of disclosure would reasonably indicate confidentiality, without any requirement for subsequent written confirmation.
- iii) The Bidder may use the Confidential Information solely for and in connection with the Purpose and shall not use the Confidential Information or any part thereof for any reason other than the Purpose stated above.

Confidential Information in oral form must be identified as confidential at the time of disclosure and confirmed as such in writing within seven (7) days of such disclosure. Confidential Information does not include information which:

- a) is or subsequently becomes legally and publicly available without breach of this Agreement by either party,
- b) was rightfully in the possession of the Bidder without any obligation of confidentiality prior to receiving it from Punjab and Sind Bank
- c) was rightfully obtained by the Bidder from a source other than Punjab and Sind Bank without any obligation of confidentiality,
- d) was developed by for the Bidder independently and without reference to any Confidential Information and such independent development can be shown by documentary evidence, or is/was disclosed pursuant to an order of a court or governmental agency as so required by such order, provided that the Bidder shall, unless prohibited by law or regulation, promptly notify Punjab &

Sind Bank of such order and afford Punjab & Sind Bank the opportunity to seek appropriate protective order relating to such disclosure.

- e) the recipient knew or had in its possession, prior to disclosure, without limitation on its confidentiality.
- f) is released from confidentiality with the prior written consent of the other party.

The recipient shall have the burden of proving hereinabove are applicable to the information in the possession of the recipient. Confidential Information shall at all times remain the sole and exclusive property of the disclosing party. Upon termination of this Agreement, Confidential Information shall be returned to the disclosing party or destroyed, if incapable of return. The destruction shall be witnessed and so recorded, in writing, by an authorized representative of each of the parties.

Nothing contained herein shall in any manner impair or affect the rights of Punjab and Sind Bank in respect of the Confidential Information.

In the event that any of the Parties hereto becomes legally compelled to disclose any Confidential Information, such Party shall give sufficient notice to the other party to enable the other Party to prevent or minimize to the extent possible, such disclosure. Neither party shall disclose to a third party any Confidential Information or the contents of this Agreement without the prior written consent of the other party. The obligations of this Clause shall be satisfied by handling Confidential Information with the same degree of care, which the receiving party applies to its own similar confidential information but in no event less than reasonable care. The obligations of this clause shall survive the expiration, cancellation or termination of this Agreement

- 5) Non-disclosure: The Bidder shall not commercially use or disclose any Confidential Information, or any materials derived there from to any other person or entity other than persons in the direct employment of the Bidder who have a need to have access to and knowledge of the Confidential Information solely for the Purpose authorized above. The Bidder shall take appropriate measures by instruction and written agreement prior to disclosure to such employees to assure against unauthorized use or disclosure. The Bidder may disclose Confidential Information to others only if the Bidder has executed a Non-Disclosure Agreement with the other party to whom it is disclosed that contains terms and conditions that are no less restrictive than these presents, and the Bidder agrees to notify Punjab & Sind Bank immediately if it learns of any use or disclosure of the Confidential Information in violation of terms of this Agreement.

Notwithstanding the marking and identification requirements above, the following categories of information shall be treated as Confidential Information under this Agreement irrespective of whether it is marked or identified as confidential:

- i) Information regarding Punjab & Sind Bank and any of its Affiliates, customers and their accounts ("Customer Information"). For purposes of this Agreement, Affiliate means a business entity now or hereafter controlled by, controlling or under common control. Control exists when an entity owns or controls more

than 10% of the outstanding shares or securities representing the right to vote for the election of directors or other managing authority of another entity; or

- ii) any aspect of Punjab and Sind Bank's business that is protected by patent, copyright, trademark, trade secret or other similar intellectual property right; or
- iii) business processes and procedures; or
- iv) current and future business plans; or
- v) personnel information; or
- vi) Financial information.

6) Publications: The Bidder shall not make news releases, public announcements, give interviews, issue or publish advertisements or publicize in any other manner whatsoever in connection with this Agreement, the contents / provisions thereof, other information relating to this Agreement, the Purpose, the Confidential Information or other matter of this Agreement, without the prior written approval of Punjab and Sind Bank.

7) Term: This Agreement shall take effect on the date of execution and shall continue for the duration of the Purpose. On completion or termination of the Purpose, the Bidder shall immediately cease use of Confidential Information and, at Punjab & Sind Bank's option, return or securely destroy it, including copies, extracts and derived material, and certify completion in writing. Retention is permitted only to the minimum extent mandatorily required by applicable law, with continued access restriction and confidentiality until secure deletion. The obligations concerning Bank Data, personal data, trade secrets, credentials and security information shall survive without time limit; other confidentiality obligations shall survive for seven (7) years after termination, without prejudice to any longer period required by law.

Any provisions of this Agreement which by their nature extend beyond its termination shall continue to be binding and applicable without limit in point in time except and until such information enters the public domain

8) Title and Proprietary Rights: Notwithstanding the disclosure of any Confidential Information by Punjab & Sind Bank to the Bidder, the title and all intellectual property and proprietary rights in the Confidential Information shall remain with Punjab and Sind Bank.

9) Remedies: The Bidder acknowledges the confidential nature of Confidential Information and that damage could result to Punjab and Sind Bank if the Bidder breaches any provision of this Agreement and agrees that, if it or any of its directors, officers or employees should engage or cause or permit any other person to engage in any act in violation of any provision hereof, Punjab & Sind Bank may suffer immediate irreparable loss for which monetary compensation may not be adequate. Punjab & Sind Bank shall be entitled, in addition to other remedies for damages & relief as may be available to it, to an injunction or similar relief prohibiting the Bidder, its directors, officers etc. from engaging in any such act which constitutes or results in breach of any of the covenants of this Agreement.

Any claim for relief to Punjab & Sind Bank shall include Punjab and Sind Bank's costs and expenses of enforcement (including the attorney's fees).

- 10) Entire Agreement, Amendment and Assignment: This Agreement constitutes the entire agreement between the Parties relating to the matters discussed herein and supersedes any and all prior oral discussions and / or written correspondence or agreements between the Parties. This Agreement may be amended or modified only with the mutual written consent of the Parties. Neither this Agreement nor any right granted hereunder shall be assignable or otherwise transferable.
- 11) Dispute Resolution: Any dispute arising out of or in connection with this Agreement shall first be referred to authorised representatives of the Parties for amicable resolution. If it remains unresolved for thirty (30) days after written notice, it shall be resolved by a sole arbitrator mutually appointed by the Parties. Failing agreement on the arbitrator within thirty (30) days, appointment shall be made in accordance with Section 11 of the Arbitration and Conciliation Act, 1996. The seat and venue shall be New Delhi, proceedings shall be in English, and courts at New Delhi shall have exclusive supervisory jurisdiction. Either Party may seek urgent interim or conservatory relief from a competent court.
- 12) Governing Law: Governing Law: The laws of India shall govern this Agreement
- 13) Jurisdiction: It is hereby agreed between the parties that any suit or legal proceedings to enforce the rights of either party under this Agreement shall be instituted and tried by a competent court in the city of Delhi only.
- 14) Authorized Signatory: The selected Bidder shall indicate the authorized signatories who can discuss and correspond with the Bank about the obligations under the contract. The selected Bidder shall submit at the time of signing the contract a certified copy of the resolution of their board, authenticated by the company secretary, authorizing an official or officials of the Bidder to discuss, sign agreements/contracts with The Bank, raise invoice and accept payments and also to correspond. The Bidder shall provide proof of signature identification for the above purposes as required by the Bank
- 15) Force Majeure: Force Majeure is herein defined as any cause, which is beyond the control of the selected Bidder or The Bank as the case may be which they could not foresee or with a reasonable amount of diligence could not have foreseen and which substantially affect the performance of the contract, such as:-
 - i) Natural phenomenon, including but not limited to floods, droughts, earthquakes, epidemics and pandemics
 - ii) Acts of any government, including but not limited to war, declared or undeclared priorities, quarantines and embargos
 - iii) Terrorist attack, public unrest in work area
 - iv) Provided either party shall within 10 days from occurrence of such a cause, notify the other in writing of such causes. The Bidder or The Bank shall not be liable for delay in performing his/her obligations resulting from any force Majeure cause as referred to and/or defined above. Any delay beyond 30 days shall lead to termination of contract by parties and all obligations expressed quantitatively shall be calculated as on date of termination.

Notwithstanding this, provisions related to indemnity, confidentiality survive termination of the contract.

- v) Unless otherwise directed by the Bank in writing, the Bidder affected by force majeure shall continue to perform the obligations under this agreement, which are not affected by the force majeure event and shall take such steps as are reasonably necessary to remove the causes resulting in force majeure and to mitigate the effect thereof.
- vi) As soon as the cause of force majeure has been removed, the Bidder shall notify the Bank and resume the affected activity without delay.
- vii) Notwithstanding the above, the decision of the Bank shall be final and binding on the Bidder in the event of force majeure.

- 16) Intellectual Property Indemnity: In the event of any claim asserted by a third party of infringement of copyright, patent, trademark, industrial design rights, etc., arising from the use of the Goods or any part thereof in India, the Vendor(s) shall act expeditiously to extinguish such claim. If the Vendor(s) fails to comply and the Bank is required to pay compensation to a third party resulting from such infringement, the Vendor(s) shall be responsible for the compensation to the claimant including all expenses, court costs and lawyer fees. The Bank will give notice to the Vendor(s) of such a claim, if it is made, without delay. The Vendor(s) shall indemnify the Bank against all third-party claims.
- 17) General: The Bidder shall not reverse - engineer, decompile, disassemble or otherwise interfere with any software disclosed hereunder.
- 18) All Confidential Information is provided "as is". In no event shall the Punjab & Sind Bank be liable for the inaccuracy or incompleteness of the Confidential Information. None of the Confidential Information disclosed by Punjab & Sind Bank constitutes any representation, warranty, assurance, guarantee or inducement with respect to the fitness of such Confidential Information for any particular purpose.
- 19) Punjab & Sind Bank discloses the Confidential Information without any representation or warranty, whether express, implied or otherwise, on truthfulness, accuracy, completeness, lawfulness, merchant ability, fitness for a particular purpose, title, non-infringement, or anything else.
- 20) Waiver: A waiver (whether express or implied) by Punjab & Sind Bank of any of the provisions of this Agreement, or of any breach or default by the Bidder in performing any of the provisions hereof, shall not constitute a continuing waiver and such waiver shall not prevent Punjab & Sind Bank from subsequently enforcing any of the subsequent breach or default by the Bidder under any of the provisions of this Agreement.

In witness whereof, the Parties hereto have executed these presents the day, month and year first herein above written.

For and on behalf of _____	For and on behalf of Punjab and Sind Bank.

Annexure 13: Commercial Proposal Submission Checklist

Instructions to be noted while preparing/submitting Part B - Commercial Proposal

All Annexure or appendix should be submitted in Bidder's Letter Head with seal and signature of the authorized signatory.

(Excel sheet uploaded in GeM along with RFP documents. File name – PSB_DPDP_BOM.xlsx)

1. Commercial Bill of Material as per Appendix 2.

Annexure 14: Bank Guarantee Format for Earnest Money Deposit

Performa for the Bank Guarantee for Earnest Money Deposit

(To be stamped in accordance with stamp act)

Ref: Bank Guarantee #

Date: _____

To

Deputy General Manager (Data Protection Office)

Punjab and Sind Bank

Second Floor, DPO Department, Corporate Office, NBCC Building Block 3,
East Kidwai Nagar, New Delhi – 110023

Dear Sir,

In accordance with your bid reference No. _____ Dated _____
M/s _____ having its registered office at _____
herein after Called „bidder”) wish to participate in the said bid for Selection of Bidder(s)
for **Reg: “Request for Proposal (RFP) for Procurement of DPDP Suite and selection
of System Integrator (SI) cum Consultant services for Supply, Installation,
Integration, Implementation and Management of Digital Personal Data Protection
Solution for a period of 3 Years”**

An irrevocable Financial Bank Guarantee (issued by a nationalized /scheduled commercial Bank) against Earnest Money Deposit amounting to Rs.....) valid up to _____ is required to be submitted by the bidder, as a condition for participation in the said bid, which amount is liable to be forfeited on happening of any contingencies mentioned in the bid document. M/s _____ having its registered office at _____ has undertaken in pursuance of their offer to Punjab & Sind Bank (hereinafter called as the beneficiary) dated _____ has expressed its intention to participate in the said bid and in terms thereof has approached us and requested us _____ (Name of Bank) _____ (Address of Bank) to issue an irrevocable financial Bank Guarantee against Earnest Money Deposit (EMD) amounting to Rs _____ (Rupees _____) valid up to _____. We, the _____ (Name of Bank) _____ (Address of Bank) having our Head office at _____ therefore Guarantee and undertake to pay immediately on first written demand by Punjab & Sind Bank ,the amount Rs _____ (Rupees _____) without any reservation, protest, demur and recourse in case the bidder fails to Comply with any condition of the bid or any violation against the terms of the bid, Without the beneficiary needing to prove or demonstrate reasons for its such demand. Any Such demand made by said beneficiary shall be conclusive and binding on us irrespective of any dispute or difference raised by the

bidder. This guarantee shall be irrevocable and shall remain valid up to _____.
If any further extension of this Guarantee is required, the same shall be extended to such required period on receiving instructions in writing, from Punjab & Sind Bank, on whose behalf guarantee is issued. "Notwithstanding anything contained herein above Our liability under this Bank guarantee shall not exceed Rs. _____ (Rupees _____).

This Bank guarantee shall be valid up to _____. We are liable to pay the guaranteed amount or any part thereof under this Bank guarantee only if you serve upon us a written claim or demand, on or before _____ 14.30 hours (Indian Standard Time) or within Bank official working hours where after it ceases to be in effect in all respects whether or not the original Bank guarantee is returned to us." In witness whereof the Bank, through its authorized officer has set its hand stamped on this _____ Day of _____ 2026 at _____

Name of signatory

Bank Common Seal

Designation

Annexure 15: Format of Performance Guarantee

(Issued by any Scheduled Commercial Bank & to be executed on stamp paper of requisite value as per stamp duty payable at place of execution.)

Tender Reference No: _____ Date _____

To

Deputy General Manager (Data Protection Office)

Punjab and Sind Bank

Second Floor, DPO Department, Corporate Office, NBCC Building Block 3,

East Kidwai Nagar, New Delhi – 110023

Dear Sir,

1. WHEREAS pursuant to a Request for Proposal dated..... (hereinafter referred to as RFP, issued by Punjab & Sind Bank, Head Office Data Protection Office Second Floor, DPO Department, Corporate Office, NBCC Building Block 3, East Kidwai Nagar, New Delhi – 110023 in response of (Bidder(s) / Service Provider), a Company registered under the Companies Act, 1956 and having its Registered / Corporate Office at has awarded the Contract valued Rs.....and appointed.....as Bidder(s) / Service Provider for procurement of **DPDP Suite and selection of System Integrator (SI) cum Consultant services for Supply, Installation, Integration, Implementation and Management of Digital Personal Data Protection Solution for a period of 3 Years**” vide Appointment letter / Purchase Order No..... dated.....on the terms and conditions as set out inter-alia in the said RFP and in the Appointment Letter / Purchase Order.
2. WHEREAS you have in terms of the said Appointment letter / Purchase Order called upon (Bidder(s) / Service Provider to furnish a Performance Guarantee, for Rs..... Rupees only), equivalent to..... of the Contract value, to be issued by a Bank in your favour towards due performance of the Contract in accordance with the specifications, terms and conditions of the said Appointment letter / Purchase Order and an Agreement entered / to be entered into in this behalf.
3. WHEREAS (Bidder(s) / Service Provider) has approached us for issuing in your favour a performance Guarantee for the sum of Rs..... (Rupees.....).

NOW THEREFORE in consideration of you having awarded the Contract to.....inter-alia on the terms & conditions that provides a performance guarantee for due performance of the terms and conditions thereof. We,.....Bank,..... a body corporate constituted under having its Head office

at.....(give full address) and a branch inter-alia
at..... India at the request of.....do hereby expressly,
irrevocably and unconditionally undertake to pay merely on demand from you and
without any demur without referring to any other source,
Rs.....(Rupees.....only) against any loss
or damage caused to or suffered by or that may be caused to or suffered by you on
account of any breach or breaches on the part of of any of the terms
and conditions of the Contract and in the event of.....committing any
default or defaults in carrying out any of the work or discharging any obligation under
the said Contract or otherwise in the observance and performance of any of the
terms and conditions relating thereto including non-execution of the Agreement as
may be claimed by you on account of breach on the part of of their
obligations or default in terms of the said Appointment letter / Purchase Order.

4. Notwithstanding anything to the contrary contained herein or elsewhere, we agree that your decision as to whether the has committed any such breach / default or defaults and the amount or amounts to which you are entitled by reasons thereof will be binding on us and we shall not be entitled to ask you to establish its claim or claims under this Guarantee, but will pay the same forthwith on demand without any protest or demur. Any such demand made by you shall be conclusive as regards the amount due and payable by us to you.
5. This Guarantee shall be valid up to plus 12 months of the Claim period from the expiry of said guarantee period. Without prejudice to your claim or claims arisen and demanded from or otherwise notified to us in writing before the expiry of the said date which will be enforceable against us notwithstanding that the same is or are enforced after the said date.
6. You will have the fullest liberty without our consent and without affecting our liabilities under this Guarantee from time to time to vary any of the terms and conditions of the said appointment letter or the Contract to be made pursuant thereto or extend the time of performance of the Contract or to postpone for any time or from time to time any of your rights or powers against the and either to enforce or forbear to enforce any of the terms and conditions of the said appointment letter or the Contract and we shall not be released from our liability under Guarantee by exercise of your liberty with reference to matters aforesaid or by reason of any time being given to or any other forbearance, act or omission on your part or any indulgence by you or any other act, matter or things whatsoever which under law relating to sureties, would but for the provisions hereof have the effect of releasing us from our liability hereunder provided always that nothing herein contained will enlarge our liability hereunder beyond the limit of Rs..... (Rupees.....only) as aforesaid or extend the period of the guarantee beyond (date) unless expressly agreed to by us in writing.

7. This Guarantee shall not in any way be affected by you are taking or giving up any securities from or any other person, firm or company on its behalf or by the winding up, dissolution, insolvency as the case may be of
8. In order to give full effect to the Guarantee herein contained, you shall be entitled to act as if we were your principal debtors in respect of all your claims against hereby guaranteed by us as aforesaid and we hereby expressly waive all our rights of surety ship and other rights, if any, which are in any way inconsistent with any of the provisions of Guarantee.
9. Subject to the maximum limit of our liability as aforesaid, this Guarantee will cover all your claim or claims against from time to time arising out of or in relation to the said appointment letter / Contract and in respect of which your claim in writing is lodged on us before expiry of Guarantee.
10. Any Notice by way of demand or otherwise hereunder may be sent by special courier, telex, fax, e-mail or registered post to our Head Office / Local address as aforesaid and if sent accordingly it shall be deemed to have been given when the same has been posted.
11. This Guarantee shall not be affected by any change in the constitution of _____ or nor shall it be affected by any change in your constitution or by any amalgamation or absorption thereof or therewith but will ensure to the benefit of and be available to and be enforceable by the absorbing or amalgamated company or concern.
12. This Guarantee shall come into force from the date of its execution and shall not be revoked by us any time during its currency without your previous consent in writing.
13. We further agree and undertake to pay you the amount demanded in writing irrespective of any dispute or controversy between you and _____ in any suit or proceeding pending before any court, Tribunal or Arbitrator relating thereto, our liability under these presents being absolute and unequivocal. The payments so made by us shall be a valid discharge of our liability for payment hereunder and _____ shall have no claim against us for making such payment.
14. We have the power to issue this Bank Guarantee in your Bank's favour as the undersigned has full power to execute this Bank Guarantee under the Power of Attorney issued by our Bank.
15. Our authority to issue this guarantee may be verified with our Controlling Office situated at _____ (full details of persons to be contacted address and phone Numbers etc).
16. Notwithstanding anything contained herein above;
 - i. Our liability under this Guarantee shall not exceed Rs _____ (Rupees _____ only)
 - ii. This Guarantee shall be valid and remain in force up to _____ plus the Claim period of 12(Twelve) months and including the date _____ and

iii. We are liable to pay the guaranteed amount or any part thereof under this Guarantee only and only if you serves upon us a written claim or demand for payment on or before the expiry of this Guarantee.

Dated this the _____ day of _____ 2026

Signature and Seal of Guarantors

Bidder(s)'s Bank

Annexure 16 : Pre-contract integrity pact

(To be stamped in accordance with stamp act)

PRE-CONTRACT INTEGRITY PACT

Between

Punjab & Sind Bank(PSB) hereinafter referred to as "The Principal",

And

_____ hereinafter referred to as "The Bidder/
Contractor"

Preamble

The Principal intends to award, under laid down organizational procedures, contract/ s for _____. The Principal values full compliance with all relevant laws of the land, rules, regulations, economic use of resources and of fairness / transparency in its relations with its Bidder(s) and / or Contractor(s).

In order to achieve these goals, the Principal has appointed **1. Sh. Debal kumar Gayen** Gayen.dk@gmail.com **2. Sh. Pramod Kumar Garg** Pkgarg.1957@gmail.com as Independent External Monitors (IEMs) who will monitor the tender process and the execution of the contract for compliance with the principles mentioned above.

Section 1 - Commitments of the Principal

(1) The Principal commits itself to take all measures necessary to prevent corruption and to observe the following principles: -

- a. No employee of the Principal, personally or through family members, will in connection with the tender for, or the execution of a contract, demand, take a promise for or accept, for self or third person, any material or immaterial benefit which the person is not legally entitled to.
- b. The Principal will, during the tender process treat all Bidder(s) with equity and reason. The Principal will in particular, before and during the tender process, provide to all Bidder(s) the same information and will not provide to any Bidder(s) confidential / additional information through which the Bidder(s) could obtain an advantage in relation to the tender process or the contract execution.
- c. The Principal will exclude from the process all known prejudiced persons.

(2) If the Principal obtains information on the conduct of any of its employees which is a criminal offence under the BNS/ IPC/PC Act, or if there be a substantive suspicion in this regard, the Principal will inform the Chief Vigilance Officer and in addition can initiate disciplinary actions

Section 2 - Commitments of the Bidder(s)/ Contractor(s)

(1) The Bidder(s)/ Contractor(s) commit themselves to take all measures necessary to prevent corruption. The Bidder(s)/ Contractor(s) commit themselves to observe the following principles during participation in the tender process and during the contract execution.

- a) The Bidder(s)/ Contractor(s) will not, directly or through any other person or firm, offer, promise or give to any of the Principal's employees involved in the tender process or the execution of the contract or to any third person any material or other benefit which he / she is not legally entitled to, in order to obtain in exchange any advantage of any kind whatsoever during the tender process or during the execution of the contract.
- b) The Bidder(s)/ Contractor(s) will not enter with other Bidders into any undisclosed agreement or understanding, whether formal or informal. This applies in particular to prices, specifications, certifications, subsidiary contract submission or non-submission of bids or any other actions to restrict competitiveness or to introduce cartelisation in the bidding process.
- c) The Bidder(s)/ Contractor(s) will not commit any offence under the relevant BNS/IPC/PC(Prevention of corruption) Act; further the Bidder(s)/ Contractor(s) will not use improperly, for purposes of competition or personal gain, or pass on to others, any information or document provided by the Principal as part of the business relationship, regarding plans, technical proposals and business details, including information contained or transmitted electronically.
- d) The Bidder(s)/Contractors(s) of foreign origin shall disclose the name and address of the Agents/representatives in India, if any, similarly the Bidder(s)/Contractors(s) of Indian Nationality shall furnish the name and address of the foreign principals, if any. Further details as mentioned in the "Guidelines on Indian Agents of Foreign Suppliers" shall be disclosed by the Bidder(s)/Contractor(s). Further, as mentioned in the Guidelines all the payments made to the Indian agent/representative have to be in Indian Rupees only.
- e) The Bidder(s)/ Contractor(s) will, when presenting their bid, disclose any and all payments made, is committed to or intends to make to agents, brokers or any other intermediaries in connection with the award of the contract.
- f) Bidder(s) /Contractor(s) who have signed the Integrity Pact shall not approach the Courts while representing the matter to IEMs and shall wait for their decision in the matter.

(2) The Bidder(s)/ Contractor(s) will not instigate third persons to commit offences outlined above or be an accessory to such offences.

Section 3 - Disqualification from tender process and exclusion from future contracts

If the Bidder(s)/Contractor(s), before award or during execution has committed a transgression through a violation of Section 2, above or in any other form such as to put their reliability or credibility in question, the Principal is entitled to disqualify the Bidder(s)/Contractor(s) from the tender process or take action as per the procedure mentioned in the "Guidelines on Banning of business dealings".

Section 4 - Compensation for Damages

(1) If the Principal has disqualified the Bidder(s) from the tender process prior to the award according to Section 3, the Principal is entitled to demand and recover the damages equivalent to Earnest Money Deposit/ Bid Security.

(2) If the Principal has terminated the contract according to Section 3, or if the Principal is entitled to terminate the contract according to Section 3, the Principal shall be entitled to demand and recover from the Contractor liquidated damages of the Contract value or the amount equivalent to Performance Bank Guarantee.

Section 5 - Previous transgression

(1) The Bidder declares that no previous transgressions occurred in the last three years with any other Company in any country conforming to the anti-corruption approach or with any Public Sector Enterprise in India that could justify his exclusion from the tender process.

(2) If the Bidder makes incorrect statement on this subject, he can be disqualified from the tender process or action can be taken as per the procedure mentioned in "Guidelines on Banning of business dealings".

Section 6 - Equal treatment of all Bidders /Contractors / Subcontractors

(1) In case of Sub-contracting, the Principal Contractor shall take the responsibility of the adoption of Integrity Pact by the Sub-contractor.

(2) The Principal will enter into agreements with identical conditions as this one with all Bidders and Contractors.

(3) The Principal will disqualify from the tender process all bidders who do not sign this Pact or violate its provisions.

Section 7 - Criminal charges against violating Bidder(s) / Contractor(s) / Subcontractor(s)

If the Principal obtains knowledge of conduct of a Bidder, Contractor or Subcontractor, or of an employee or a representative or an associate of a Bidder, Contractor or Subcontractor which constitutes corruption, or if the Principal has substantive suspicion in this regard, the Principal will inform the same to the Chief Vigilance Officer.

Section 8 - Independent External Monitor

(1) The Principal appoints competent and credible Independent External Monitor for this Pact after approval by Central Vigilance Commission. The task of the Monitor is to review independently and objectively, whether and to what extent the parties comply with the obligations under this agreement.

(2) The Monitor is not subject to instructions by the representatives of the parties and performs his/her functions neutrally and independently. The Monitor would have access to all Contract documents, whenever required. It will be obligatory for him / her to treat the information and documents of the Bidders/Contractors as confidential. He/ she reports to the MD & CEO of Punjab and Sind Bank.

(3) The Bidder(s)/Contractor(s) accepts that the Monitor has the right to access without restriction to all Project documentation of the Principal including that provided by the Contractor. The Contractor will also grant the Monitor, upon his/her request and demonstration of a valid interest, unrestricted and unconditional access to their project documentation. The same is applicable to Sub-contractors.

(4) The Monitor is under contractual obligation to treat the information and documents of the Bidder(s)/ Contractor(s)/ Sub-contractor(s) with confidentiality. The Monitor has also signed declarations on 'Non-Disclosure of Confidential Information' and of 'Absence of Conflict of Interest'. In case of any conflict of interest arising at a later date, the IEM shall inform MD & CEO of Punjab & Sind Bank and recuse himself / herself from that case.

(5) The Principal will provide to the Monitor sufficient information about all meetings among the parties related to the Project provided such meetings could have an impact on the contractual relations between the Principal and the Contractor. The parties offer to the Monitor the option to participate in such meetings.

(6) As soon as the Monitor notices, or believes to notice, a violation of this agreement, he/she will so inform the Management of the Principal and request the Management to

discontinue or take corrective action, or to take other relevant action. The monitor can in this regard submit non-binding recommendations. Beyond this, the Monitor has no right to demand from the parties that they act in a specific manner, refrain from action or tolerate action.

(7) The Monitor will submit a written report to the MD & CEO of Punjab and Sind Bank, within 8 to 10 weeks from the date of reference or intimation to him by the Principal and, should the occasion arise, submit proposals for correcting problematic situations.

(8) If the Monitor has reported to the MD & CEO of Punjab & Sind Bank, a substantiated suspicion of an offence under relevant BNS/ IPC/ PC Act, and the MD & CEO of Punjab & Sind Bank has not, within the reasonable time taken visible action to proceed against such offence or reported it to the Chief Vigilance Officer, the Monitor may also transmit this information directly to the Central Vigilance Commissioner.

(9) The word 'Monitor' would include both singular and plural

Section 9 - Pact Duration

This Pact begins when both parties have legally signed it. It expires for the Contractor 12 months after the last payment under the contract, and for all other Bidders 6 months after the contract has been awarded. Any violation of the same would entail disqualification of the bidders and exclusion from future business dealings.

If any claim is made / lodged during this time, the same shall be binding and continue to be valid despite the lapse of this pact as specified above, unless it is discharged / determined by MD & CEO of Punjab and Sind Bank.

Section 10 - Other provisions

(1) This agreement is subject to Indian Law. Place of performance and jurisdiction is the Registered Office of the Principal, i.e. New Delhi.

(2) Changes and supplements as well as termination notices need to be made in writing. Side agreements have not been made.

(3) If the Contractor is a partnership or a consortium, this agreement must be signed by all partners or consortium members.

(4) Should one or several provisions of this agreement turn out to be invalid, the remainder of this agreement remains valid. In this case, the parties will strive to come to an agreement to their original intentions.

(5) Issues like Warranty / Guarantee etc. shall be outside the purview of IEMs.

(6) In the event of any contradiction between the Integrity Pact and its Annexure, the Clause in the Integrity Pact will prevail.

(For & On behalf of the Principal)
Contractor)

(For & On behalf of Bidder /

Place -----

Date -----

Witness 1:

(Name & Address)

Witness 2:

(Name & Address)

Annexure 17: Compliance with Scope of Work and SBOM

RFP No:

(Letter to be submitted by the OEM's on their letter head)

To

Deputy General Manager (Data Protection Office)

Punjab and Sind Bank

Second Floor, DPO Department, Corporate Office, NBCC Building Block 3,
East Kidwai Nagar, New Delhi – 110023

Dear Sir,

Sub: Reg: Request for Proposal (RFP) for Procurement of DPDP Suite and selection of System Integrator (SI) cum Consultant services for Supply, Installation, Integration, Implementation and Management of Digital Personal Data Protection Solution for a period of 3 Years vide RFP No: _____

We, who are established and reputable manufacturers / producers of _____ having factories / development facilities at _____ (address of factory / facility) confirms the following:

S.No.	Product name as per RFP	Product name as per OEM

1. We confirm that we comply with the FRS & TRS requirement **(the requirement being met through our standard features available in our product)** stated in the RFP and are attaching the Excel/PDF of compliance
2. We confirm that we comply with the SoW requirement stated in the RFP for our product.
3. We have attached the Software Bill of Materials (SBOM) and Cryptography Bill of Materials (CBOM - Public) for the proposed solution in the format prescribed under Annexure 18. The detailed/private SBOM and CBOM containing confidential or sensitive security information shall be provided to the Bank after issuance of the Purchase Order and execution of applicable confidentiality requirements.
4. We further confirm that we support secure, automated, and machine-readable exchange of SBOM/CBOM information through industry-recognized formats and mechanisms and shall facilitate the Bank in obtaining updated SBOM/CBOM information throughout the contract period.
5. We undertake to provide all necessary OEM support, software updates, security patches, vulnerability disclosures, technical advisories, and product lifecycle information for the duration of the contract.

6. We understand that any misrepresentation, incorrect declaration, or inconsistency between this declaration, the bidder's submission, the Undertaking, or the proposed products may result in rejection of the bid and/or any action deemed appropriate by the Bank.

Yours faithfully
Authorized Signatory
(Name of manufacturers):

Place:
Name:
Date:
Phone No.:
Fax:
E-mail:

Annexure 18: S-BOM & C-BOM details of all the proposed Tool/solutions

a. S-BOM

On OEM Letterhead

Sr. No.	Component	Component Name	Component Name	Component Name	Component Name
1.	Version				
2.	Description				
3.	Supplier				
4.	License				
5.	Origin				
6.	Dependencies				
7.	Vulnerabilities				
8.	Patch Status				
9.	Release Date				
10.	End of Life Date				
11.	Usage Restrictions				
12.	Checksums				
13.	Hashes				
14.	Executable Property				
15.	Archive Property				
16.	Structured Property				
17.	Unique Identifier				

b. C-BOM

On OEM Letterhead

Cryptographic Asset Type	Element	Description	Details to be furnished by Bidder
Algorithms	Name	The name of the cryptographic algorithm or asset (e.g., "AES-128-GCM").	
	Asset Type	Specifies the type of cryptographic asset (for algorithms, this is "algorithm").	
	Primitive	Describes the cryptographic primitive used (e.g., "signature" for SHA512withRSA).	
	Mode	The operational mode used by the algorithm (e.g., "gcm" for Galois/Counter Mode).	
	Crypto Functions	The specific cryptographic functions supported, such as key generation, encryption, decryption, and authentication tag generation.	
	Classical security level	The strength of the asset against classical (non-quantum) attacks, measured in bits (e.g., 128 bits for AES-128).	
	OID	The globally unique Object Identifier used to refer to the algorithm across different systems (e.g., "2.16.840.1.101.3.4.1.6" for AES-128-GCM).	
	List	A list of cryptographic algorithms employed by the system to assess security capabilities and post-quantum encryption standards.	
Keys	Name	A unique identifier or name for the key used in cryptographic operations.	
	Asset Type	Defines the type of cryptographic asset (typically "key").	
	Id	A unique reference number or key ID.	
	State	The current operational state of the key, such as active, revoked, or expired.	
	Size	The size of the key, typically measured in bits (e.g., a 128-bit key or a 2048-bit RSA key).	
	Creation Date	The date when the key was originally created.	
	Activation Date	The date when the key became operational or was first used.	
Protocols	Name	The name of the cryptographic protocol (e.g., TLS, IPsec, SSH).	
	Asset Type	Defines the type of cryptographic asset (in this case, "protocol").	

	Version	The specific version of the protocol used (e.g., TLS 1.2, TLS 1.3).	
	Cipher Suites	The set of cryptographic algorithms and parameters supported by the protocol for encryption, key exchange, and integrity checking.	
	OID	The Object Identifier associated with the protocol to identify its unique specifications.	
Certificates	Name	The name of the certificate, typically referring to its subject or the entity it represents.*	

Annexure 19: Minimum Local Content Certification

Format for Affidavit of Self certification regarding Local Content in line with PPP-MII order and MoP Order, if applicable, to be provided on a non-judicial stamp paper of Rs. 100/-.

TENDER REREFERENCE NUMBER: _____

Date:

To

Deputy General Manager (Data Protection Office)

Punjab and Sind Bank

Second Floor, DPO Department, Corporate Office, NBCC Building Block 3,

East Kidwai Nagar, New Delhi – 110023

Dear Sir,

- This is to certify that proposed is having the local content of % as defined in the RFP.
- This certificate is submitted in reference to the Public Procurement (Preference to Make in India), Order 2017 – Revision vide Order No. P-45021/2/2017-PP (BE-II) dated 19 Jul ,2024.
- _____(Details of Locations where value additions are made).

Signature of Authorized Signatory

Name:

Date:

Designation:

Seal:

Annexure 20 Client References Format

Format for Submission of Client References

To whosoever it may concern

Particulars	Details
Client Information	
Client Name	
Client address	
Name of the contact person and designation	
Phone number of the contact person	
E-mail address of the contact person	
Project Details	
Name of the Project	
Start Date of the project	
End Date of the project	
Current Status (In Progress / Completed)	
Size of Project	
Value of Work Order (In Lakh) (only single work order)	
Scope of work	
Brief Scope of work relevant to the Bank's (PSB) RFP Requirement	
DPDP Solution Integration done for out of the below 1. CBS 2. ITSM (Manage Engine) 3. Network/ NOC 4. SIEM/SOC 5. UPI 6. IMPS 7. AEPS 8. LOS 9. Any other Upstream/ Downstream application / touchpoint (Please specify)	
Name and Version of Solution	
No. of Branches/offices	
Supporting Document to substantiate the Scope of work	Contract Copy/PO/Credential letter/ Email Confirmation/ Self Declaration (for OEMs)

Name & Signature of authorised signatory

Date

Place

Seal of Company

Annexure 21: Pre-bid Query format

Pre-Bid Query Format

(Bidders should submit the queries in excel format only)

Ref: RFP No. _____ dated _____.

Bidder's Name: _____

S.No.	Page No.	Section	RFP Clause	Clause/Technical Specification	Bidder's Query
1					
2					
3					
4					
5					

- Add as many rows as required

Annexure 22: Proposed Resources CV

Sr No	Parameter	Description
1	Name & Designation	
2	Proposed Position & Skillset	
3	Educational Qualification	
	Degree Obtained	University/ Institution
		Year Obtained
4	Privacy Certification/ Qualifications as mentioned in RFP	
5	Professional Experience	
	Designation	Company Name
		Year Obtained
6	Total Years of Privacy or Data Protection Experience	
7	DPDP Solution Integration done for out of the below 1. CBS 2. ITSM (Manage Engine) 3. Network/ NOC 4. SIEM/SOC 5. UPI 6. IMPS 7. AEPS 8. LOS 9. Any other Upstream/ Downstream application / touchpoint (Please specify)	
8	Experience relevant to the Project Wise	

Annexure 23: Undertaking for Being the OEM/OSD of the Offered Primary Product

(To be provided on the Letter head of the OEM/OSD duly signed & stamped by their Authorized Signatory)

To
Deputy General Manager (Data Protection Office)
Punjab and Sind Bank
Second Floor, DPO Department, Corporate Office, NBCC Building Block 3,
East Kidwai Nagar, New Delhi – 110023

Sir,
Reg.: Procurement of DPDP Suite and selection of System Integrator (SI) cum consultant services for Supply, Installation, Integration, Implementation and Management of Digital Personal Data Protection Solution for a period of 3 Years

We hereby submit the following: -

We, M/s _____ are the OEM/OSD of the devices/components/solution/ services (as per Table A) having factories/Offices at _____ do hereby offer our quotation against the above bid invitation with our products.

Sr. No.	Hardware/Solution/ Component/ Software/Services Name	Model No./ Version No. and Release Date	Hardware/Software, component/ services/ licenses conform to all the technical specifications and requirements mentioned in this RFP (Yes/No)

(Add as many rows as required)

We hereby extend our guarantee and warranty as per the terms and conditions of this RFP and its subsequent Corrigendum and/or Clarifications, if any, and the contract for the equipment/component/solution/device and services offered against this invitation. In case of default/non-compliance of the IT asset supplied including hardware / software as per RFP requirements during the contract period, we agree to replace the IT asset including hardware / software supplied with new one in accordance with RFP requirements. We also hereby undertake to fulfil the obligations as set out in the RFP in respect of such equipment and services. With reference to all the components/parts/assemble/software used inside the company products being quoted by us vide your tender cited above, we hereby undertake that all the components / parts / assembly used inside the company products/software shall be original new components / parts / assembly / software only and that no refurbished, duplicate, second-hand components, parts, assembly are being supplied.

Yours faithfully,
Signature of Authorized Signatory
Name of Signatory:
Designation:
Email ID/ Mobile No:
Seal of Company: