Request for Proposal (RFP)

for

Provision of DPDP Program Manager

RFP: IT-26-27-262
Date: 14-11-2026

This document is the property of Multi Commodity Exchange of India Ltd (MCX). It may not be copied, distributed, or recorded on any medium, electronic, or otherwise, without MCX written permission. Use of contents given in this document, even by the authorized personnel/agencies for any other purpose other than the purpose specified herein, is strictly prohibited as it shall amount to copyright violation and thus shall be punishable under the Indian law

1. INTRODUCTION:

Multi Commodity Exchange of India Limited (MCX), India's first listed exchange, is a state-of-the- art, commodity derivatives exchange that facilitates online trading of commodity derivatives transactions, thereby providing a platform for price discovery and risk management. The Exchange, which started operations in November 2003, operates under the regulatory framework of Securities and Exchange Board of India (SEBI). Multi Commodity Exchange Clearing Corporation Ltd. (MCXCCL) is a wholly owned subsidiary of Multi Commodity Exchange of India Ltd (MCX), as a Clearing Corporation.

Considering regulatory requirements in India (SEBI, CERT-In, NCIIPC etc.) and increasing innovative cyber risk threats, malwares and threats emanating from emerging technologies MCX & MCXCCL (hereinafter referred to as "MCX Group") have implemented Cyber Security technologies.

2. OBJECTIVE:

MCX intends to engage an experienced Data Privacy Professional as a dedicated DPDP Privacy Program Manager for a period of six months.
The selected professional shall be responsible for driving the successful implementation of Digital Personal Data Protection Act, 2023 (DPDP Act), the Digital Personal Data Protection Rules, 2025compliance across MCX, covering regulatory, operational, contractual, technology and governance requirements.
The engagement requires hands-on privacy expertise, independent assessment, proactive identification of implementation gaps, stakeholder engagement and end-to-end execution of the compliance roadmap.
The resource shall be expected to identify and address detailed implementation requirements, including operational nuances, exceptions, dependencies and scenarios that may not have been explicitly identified in the existing implementation plan.
The engagement shall be outcome-driven, with emphasis on operational implementation, closure of compliance gaps and demonstrable compliance readiness.

3. DETAILED REQUIREMENTS / SCOPE OF WORK (SoW)

3.1 DPDP Program Manager:

The selected bidder shall provide experienced professional resources to undertake end-to-end program management, implementation coordination, monitoring and governance of MCX's DPDP compliance initiatives. The engagement shall cover the following activities, including but not limited to:

- Assess the existing DPDP implementation status (in support with existing team) and identify outstanding regulatory, operational, contractual, process and technology requirements.
- Develop and execute a comprehensive implementation roadmap covering all applicable DPDP compliance requirements.
- Identify detailed implementation scenarios, exceptions, dependencies and gaps across business functions, applications, processes and third-party arrangements.
- Translate regulatory requirements into actionable controls, operating procedures, system requirements and measurable deliverables.
- Drive implementation of privacy notices, Data Principal rights, grievance redressal,

Public

privacy governance and applicable consent requirements.

- Ensure appropriate treatment of personal data across collection, processing, sharing, storage, retention and deletion.
- Address requirements relating to children's personal data, legacy personal data, applicable exemptions and regulatory retention obligations.
- Ensure compliance requirements are appropriately implemented across relevant MCX business functions, applications, Member interfaces and third-party integrations.
- Assess personal data processing and sharing across the trading lifecycle, including UCC registration, transaction processing, clearing and settlement interfaces, and interactions between MCX, Trading Members, MCXCCL and other relevant stakeholders.
- Identify and drive closure of privacy compliance gaps arising from Member-facing applications, APIs, system integrations and data-sharing arrangements, considering the respective roles and responsibilities of MCX and other ecosystem participants.
- Assess personal data processing across the employee lifecycle, including recruitment, onboarding, payroll, benefits, performance management, background verification and separation.
- Drive implementation of privacy requirements for employees, prospective employees, former employees and contractual workforce, including appropriate notices and lawful processing grounds.
- Assess privacy requirements relating to HR applications, payroll providers, recruitment agencies, background verification agencies, insurers and other service providers.
- Identify and address requirements relating to employee data sharing, monitoring, cross-border transfers, retention, archival and deletion, considering applicable statutory and regulatory obligations.
- Ensure operational readiness for applicable employee Data Principal rights and grievance redressal mechanisms. Coordinate with HR, IT, Information Security and relevant stakeholders to implement and validate employee data protection controls.

Privacy Enhancing Technologies (PETs) and Data Protection Controls

- Assess the applicability of Privacy Enhancing Technologies (PETs) across MCX systems and personal data processing activities.
- Identify requirements relating to data masking, pseudonymisation, tokenisation, encryption, anonymisation and other relevant privacy protection techniques.
- Coordinate implementation of approved PETs and validate their effectiveness in consultation with IT, Information Security and relevant stakeholders.
- Drive implementation of privacy management capabilities, including data discovery, classification, RoPA, DPIA and data retention and deletion management.
- Identify privacy risks arising from data flows, system integrations, third-party processing and existing business processes.
- Ensure appropriate privacy controls are incorporated into operational processes and technology implementations.

Consent Management Solution Implementation

- Drive end-to-end implementation of the consent management solution, including requirements finalisation, vendor coordination, configuration, integration, testing, UAT and production rollout.
- Identify/ assist to identify consent requirements across applicable MCX applications, websites, Member interfaces and business processes.

Public

- Ensure implementation of consent capture, notice presentation, consent records, withdrawal mechanisms, preference management and audit trails, wherever applicable.
- Identify and address complex implementation scenarios, including legacy data, consent withdrawal propagation, third-party data sharing and applicable exemptions.
- Coordinate with IT, application owners, Members and solution providers to ensure successful integration with relevant systems.
- Review functional requirements, configurations, test scenarios and UAT outcomes from a privacy compliance perspective.
- Drive closure of identified gaps and validate operational readiness before production deployment.

Data Processing Agreements with Members and Vendors

- Drive end-to-end implementation of the DPA program covering applicable Members, vendors, service providers and other relevant third parties.
- Identify and validate entities requiring DPAs based on processing activities, contractual relationships and applicable regulatory requirements.
- Coordinate finalisation of DPA templates with MCX Legal, Data Privacy and relevant stakeholders.
- Develop and execute a structured rollout plan covering communication, engagement, negotiations, execution and closure.
- Identify common Members across exchanges and facilitate industry-level coordination, wherever appropriate.
- Address contractual and operational requirements relating to data processing roles, processing instructions, subprocessors, data sharing, retention, breach notification and other applicable obligations.
- Maintain a consolidated DPA tracker covering applicability, communication, negotiations, execution status, exceptions and pending actions.
- Drive timely execution of applicable DPAs and escalate unresolved contractual or operational dependencies.
- Ensure executed agreements and supporting records are appropriately maintained.

Data Discovery, RoPA, DPIA and Data Lifecycle Management

- Track completion of personal data discovery across applicable endpoints, databases, servers, applications and network repositories.
- Coordinate / review identification and mapping of personal data flows, processing purposes, data categories, recipients and relevant third parties.
- Review and drive completion of RoPA across applicable business functions.
- Identify processing activities requiring DPIAs and coordinate their completion and closure of identified privacy risks.
- Assess data retention and deletion requirements, including applicable statutory, regulatory and business retention obligations.
- Coordinate implementation of approved retention, archival and deletion controls.
- Ensure data discovery findings are appropriately reconciled with RoPA, DPIA and other compliance records.

Data Principal Rights and Breach Management

- Drive implementation of operational mechanisms for handling applicable Data Principal rights, including access to information, correction, erasure, grievance redressal and nomination.
- Identify requirements relating to request authentication, workflow ownership, response handling, escalation and recordkeeping.

Public

- Coordinate implementation of personal data breach management processes, including detection, assessment, escalation, notification and documentation.
- Ensure relevant operational procedures, responsibilities and communication mechanisms are established.
- Validate implementation through process walkthroughs, testing and supporting evidence.

Stakeholder Management

- Engage with Heads of Departments, business functions, IT, Information Security, Legal, HR, Procurement and Trading members and other relevant stakeholders.
- Drive closure of function-wise compliance deliverables through active engagement and follow-up.
- Identify interdepartmental dependencies and proactively facilitate their resolution.
- Escalate unresolved issues, resource constraints and implementation delays with recommended corrective actions.

.**Program Governance and Reporting**

- Maintain an integrated implementation plan covering workstreams, milestones, responsibilities, dependencies and target dates.
- Maintain consolidated action trackers, risk registers, issue logs, dependency registers and decision records.
- Provide weekly progress reports covering implementation status, completed activities, upcoming milestones and critical dependencies.
- Prepare monthly management dashboards and presentations.
- Proactively identify implementation delays and drive corrective actions.
- Maintain a consolidated repository of implementation documentation and compliance evidence.
- Ensure appropriate knowledge transfer and structured handover at the conclusion of the engagement.

3.MINIMUM QUALIFICATION & EXPERIENCE REQUIRMENTS

- The proposed resource shall be an experienced privacy professional with demonstrated expertise in implementing enterprise-wide data protection compliance programs.
- Essential Requirements
- Minimum 10 years of relevant professional experience, including at least 5 years in data privacy, data protection or privacy compliance implementation.
- Strong working knowledge of the DPDP Act, 2023, applicable Rules and associated compliance requirements.
- Demonstrated experience in end-to-end implementation of enterprise-wide privacy compliance programs.
- Practical knowledge of GDPR and internationally recognised privacy management practices.
- Hands-on experience in consent management, PETs, RoPA, DPIA, data discovery, retention, deletion, Data Principal rights and third-party governance.
- Experience in implementing privacy technology solutions and translating regulatory requirements into functional and technical specifications.
- Ability to independently identify granular implementation requirements, operational exceptions and complex data processing scenarios.
- Strong understanding of enterprise applications, data flows, third-party integrations

Public

and technology dependencies.
- Experience in managing cross-functional implementation programs involving business stakeholders, technology teams and external vendors.
- Strong analytical, problem-solving, communication, stakeholder management and execution capabilities.
- Preferred Qualifications
- Experience in stock exchanges, commodity exchanges, clearing corporations, depositories, banks or other regulated financial institutions.
- Relevant privacy certifications such as CIPP/E, CIPM, CIPT, DCPP or equivalent.
- PMP, PRINCE2 or equivalent project/program management certification.
- Prior experience in successfully delivering regulatory compliance programs involving multiple business functions and technology platforms.

4. CONFIDENTIALITY, DATA PROTECTION & OWNERSHIP

The bidder and the deployed resource shall maintain strict confidentiality concerning all personal data, non-public information, trading-related information, business records, system details and other confidential information accessed during the engagement.
The bidder shall ensure that:

- Personal data is accessed only on a need-to-know and authorised basis.
- Information is processed solely for the purposes permitted under the contract and the Exchange's instructions.
- Personal data is not transferred to unauthorised systems, personal devices, external storage media or unapproved cloud services.
- All incidents involving suspected unauthorised access, disclosure, copying, loss or misuse of information are reported immediately through the Exchange's prescribed channels.
- Access credentials, documents and other Exchange assets are returned or disabled upon termination of the engagement or withdrawal of access.
- Confidentiality and applicable data protection obligations continue after completion or termination of the contract, to the extent required by the contract and applicable law.
  All Exchange-specific deliverables, documentation, compliance records and work products created under the engagement shall belong to the Exchange, subject to the terms of the contract and applicable law.

5. DURATION & REVIEW OF ENGAGEMENT

- The engagement shall be for a period of six months from the agreed commencement date.
- The selected bidder shall deploy one dedicated, full-time Program Manager.
- The resource shall be deployed onsite at the MCX office in Mumbai on all MCX working days, in accordance with MCX working hours and attendance requirements.
- Remote or hybrid working shall not be permitted unless specifically authorised by MCX.
- The resource shall work under the overall direction of the MCX Data Privacy function.
- The resource shall actively participate in implementation activities and shall not function solely as a reporting or coordination resource.
- The selected bidder shall ensure continuity of the deployed resource throughout the engagement.
- Any replacement shall require prior written concurrence from MCX and appropriate

Public

knowledge transfer.

- The engagement may be extended based on program requirements and mutual agreement.

6. SELECTION WEIGHTAGE CFRITERIA

Technical 70% - Commercial 30% (Threshold for Technical Selection – 55 out of 70)

TECHNICAL EVALUATION CRITERIA

S.No	Evaluation Area	Weightage
1	Privacy Subject Matter Expertise: Practical knowledge of DPDP, Consent management, PETs, DPIA, ROPA n third party privacy requirements	30%
2	Program Management and Execution Capabilities : Ability to independently run a program, manage stakeholders, drive deliverables and achieve compliance readiness	30%
3	Relevant Experience: proven experience in delivering enterprise wide privacy compliance programs	10%
	Technical Evaluation Weightage	**70%**
	Commercial Evaluation Weightage	**30%**
	Total	**100%**

7. VENDOR REQUIRMENTS & SERVICE LEVEL AGREEMENTS (SLA)

- The selected resource shall be responsible for proactively driving the successful implementation of the DPDP compliance program.
- The resource shall:
- Independently identify applicable requirements, implementation gaps and operational dependencies.
- Take ownership of driving agreed compliance deliverables to completion.
- Identify requirements and implementation scenarios not explicitly captured in the existing roadmap.
- Ensure compliance requirements are translated into operational processes, technical controls and contractual arrangements.
- Drive closure of identified gaps through direct engagement with responsible stakeholders.
- Validate implementation outcomes and maintain supporting evidence.
- Escalate critical risks and unresolved dependencies with actionable recommendations.
- Demonstrate measurable compliance progress against agreed milestones.
- The resource shall be accountable for the completeness and quality of implementation assessments, proactive identification of requirements, execution management and

Public

validation of agreed deliverables.

- MCX shall retain final authority over regulatory interpretations, risk acceptance, contractual approvals, policy approvals and formal compliance sign-off.

Performance Evaluation and Acceptance

Performance shall be evaluated against:

- Achievement of agreed implementation milestones.
- Completeness of regulatory applicability and gap assessments.
- Identification and resolution of granular implementation requirements.
- Successful implementation and operational readiness of the consent management solution.
- Progress and closure of applicable DPAs with Members and vendors.
- Implementation and validation of applicable PETs and privacy controls.
- Completion and validation of data discovery, RoPA, DPIA and other privacy workstreams.
- Timely closure of compliance gaps and dependencies.
- Quality and completeness of implementation evidence.
- Effectiveness of stakeholder engagement and issue resolution.
- Demonstrated compliance readiness and successful handover.
- Submission of status reports, trackers or meeting records alone shall not constitute satisfactory delivery.

- **Non Disclosure Agreement (NDA)**
  Successful Bidder must sign NDA just after receiving the PO, pledging to safeguard the security & privacy during the time of engagement as well as post the discontinuance of business engagement for the stipulated period as per NDA requirements.

Period of Engagement – 6 months Days

Annexure - E: Commercial Format

Sr. No.	Description	Unit	Total in INR
1	Professional services for DPDP Program Manager	01	
Taxes Extra			

8. **Payment Terms:**
   Payment will be released on quarterly basis post satisfactory service delivery and signoff by MCX IS team.

Public

Annexure–F: Notification, Confidentiality, Termination Clause

Notification:

MCX Group may in its absolute discretion apply selection criteria specified in the document for evaluation of proposals for short listing / selecting the eligible Bidder. MCX Group is not obliged to provide any reasons for any such acceptance or rejection as evaluation process in entirely internal.

The Exchange reserves the right to amend or modify the contents of RFP at any time before the date of bids submission. The decision of the Management Committee of MCX Group shall be final Submission of proposal notifies deemed acceptance of terms as mentioned in this RFP by Bidder.

Confidentiality:

The RFP document is strictly confidential and is not to be disclosed, reproduced, published in any manner, transmitted, or otherwise made available by the Recipient to any other party. MCX Group may update or revise the RFP document or any part of it at its sole discretion. The Recipient acknowledges that any such revised or amended document received by it shall be subject to the same terms and conditions as this original and subject to the same confidentiality undertaking. All Information pertaining to the Exchange obtained by the Service Provider because of participation in this RFP / project is confidential and must not be disclosed without prior written authorization from the Exchange.

Termination Clause:

If the product / solution / services are not found to be satisfactory or if any non- compliance in product / service with respect to RFP or breach of delivery terms, SLA, uptime then MCX Group reserves the right to terminate the contract / Purchase Order (PO) giving notice to the bidder. The bidder should refund the payment made by MCX Group, if any.

If delivery and services are not completed within as per project timelines, MCX Group reserves the right to terminate the PO. The bidder should refund the payment made by MCX Group if any.

This document is the property of Multi Commodity Exchange of India Ltd (MCX). It may not be copied, distributed, or recorded on any medium, electronic, or otherwise, without MCX written permission. Use of contents given in this document, even by the authorized personnel/agencies for any other purpose other than the purpose specified herein, is strictly prohibited as it shall amount to copyright violation and thus shall be punishable under the Indian law

Annexure H: IT Act & Free from Malware/Backdoor Certificate (If applicable)

Information Technology Act Clause – Free of Malware/Backdoor/Harmful code

10.1 The Vendor understands and acknowledges that certain systems/computer resources/equipment/setups of MCX are identified as a Critical Information Infrastructure ("CII"). Therefore, All the Laws/ rules/ regulations and guidelines applicable to CII's and Protected Systems including the *"Information Technology Act, 2000"* and *"Information Security Practices and Procedures for Protected Systems",* set out in Gazette notification dated 22nd May 2018, shall be applicable to MCX.

10.2 The Vendor represents and warrants that: (1) the Vendor and/or its personnels shall always comply with the required laws, regulations and guidelines, applicable to the them, to ensure safety and security of MCX's CII's and Protected Systems; (2) the Vendor and/or its personnels shall not damage/harm MCX's systems/computer resources/equipment/setups; (3) the Vendor and/or its personnels shall not try to obtain unauthorized access to MCX's systems/computer resources/equipment/setups; (4) Vendor and/or its personnels shall not plant or place any harmful code, virus, self-propagating program, Trojan horse, trap door, backdoors or any other kind of harmful code or program in MCX's systems/computer resources/equipment/setups; (5) The Vendor and its personnel shall not leak and/or misuse the information stored and available on MCX's systems/computer resources/equipment/setups. Furthermore, the Vendor agrees to indemnify and keep indemnified, hold harmless and defend MCX against any/all loss, claims damage and penalty, that may be incurred by MCX, due to breach of Vendor's representations and warranties, as mentioned in this provision. In addition to the above the Vendor may also be liable for the punishment and/or penalty prescribed under the applicable laws (including of Information Technology Act, 2000)

This document is the property of Multi Commodity Exchange of India Ltd (MCX). It may not be copied, distributed, or recorded on any medium, electronic, or otherwise, without MCX written permission. Use of contents given in this document, even by the authorized personnel/agencies for any other purpose other than the purpose specified herein, is strictly prohibited as it shall amount to copyright violation and thus shall be punishable under the Indian law