H.P. STATE ELECTRONICS DEVELOPMENT CORPORATION LTD.

(A Unit of H.P. Government Undertaking)

REQUEST FOR PROPOSAL (RFP) FOR EMPANELMENT OF AGENCIES TO PROVIDE END TO END DPDP COMPLIANCE SERVICES ON BEHALF OF VARIOUS GOVT. DEPARTMENTS/ORGANIZATIONS.

(E- tender No.: HPSEDC/HP/2026-27/3372)

H.P. STATE ELECTRONICS DEVELOPMENT CORPORATION LTD.,
1st FLOOR, I.T BHAWAN, MEHLI, SHIMLA-171013, H.P.
Tel. Nos.: 0177-2623259, 2623043, 2623513 (Telefax): 0177-2626320.
Email: hpsedc@hpsedc.in

Website: www.hpsedc.in, tender document can also be downloaded from https://hptenders.gov.in

Contents

IMPORTANT INFORMATION

<table>
<tr><td>1.</td><td>Tender Inviting Authority Designation and Address</td><td>H.P State Electronics Development Corporation Limited Regd. 1st Floor, I.T. Bhawan, Mehli, Shimla-171013</td></tr>
<tr><td rowspan="3">2.</td><td>Name of the Work</td><td>Rate Contract of Empanelment of Agencies to provide end to end DPDP Compliance Services on behalf of various Govt. Departments/Organizations</td></tr>
<tr><td>Tender reference</td><td>HPSEDC/HP/2026-27/3372</td></tr>
<tr><td>Place of Execution</td><td>Entire Himachal Pradesh</td></tr>
<tr><td>3.</td><td>Tender document availability</td><td>Tender Document is available at www.hpsedc.in & hptenders.gov.in from 22/09/2026</td></tr>
<tr><td></td><td>Processing Fee for Tender</td><td>The bidder shall pay non-refundable tender document fee & eService fees through Online Mode (Available on NIC Procurement Portal). Scanned copy of Online Payment Receipt should be uploaded along with technical bid. The details of the payment to be paid is given as under: -
<table>
<tr><th>S#</th><th>descriptions</th><th>Amount</th><th>GST @18%</th><th>Total</th></tr>
<tr><td>1.</td><td>Tender document fee</td><td>10000.00</td><td>1800.00</td><td>11800.00</td></tr>
<tr><td>2.</td><td>eService Fee</td><td>1000.00</td><td>180.00</td><td>1180.00</td></tr>
<tr><td></td><td></td><td></td><td>Total</td><td>12980.00</td></tr>
</table></td></tr>
<tr><td></td><td>Earnest Money Deposit (EMD)</td><td>The Payment for EMD (refundable) of 1,00,000/- (Rupees One Lakh only) can be made by eligible bidders through Online Mode Available on NIC Procurement Portal). Scanned copy of Online Payment Receipt should be uploaded along with technical bid.

Note: As per Notification No. 4-Ind/SP/Misc/F6-10/4/80-Vol-V dated 16.05.2020 issued by Controller of Stores Himachal Pradesh or any other orders issued by Govt. of Himachal Pradesh, a bidder may be granted exemption in tender fee and EMD provided it meets either of the below mentioned criteria:
• The bidder is registered with the State Store Purchase Organization, or
• Bidder is registered with NSIC.
The bidder shall submit either of the above-mentioned certificates to avail exemption from EMD and Tender Fee.</td></tr>
<tr><td>4.</td><td>Starting date of Bid Submission</td><td>05/10/2026 from 02.00 PM onwards</td></tr>
<tr><td>5.</td><td>Performance Security</td><td>5% of order value per department engagement to be submitted within 15 days of confirmation of the work order</td></tr>
<tr><td>6.</td><td>Pre-bid meeting</td><td>The pre-bid meeting will be held on 30/09/2026 at 11:30 PM in conference room HPSEDC,1st Floor, I.T Bhawan, Mehli Shimla. The pre-bid queries in writing should be submitted before 29/09/2026 by 5.00 PM. After due date and time, no pre-bid queries will be entertained. Video Conferencing Link is as under: https://meet.google.com/fyb-dmia-vsj</td></tr>
<tr><td>7.</td><td>Last date and time for bid submission (Online Mode only on e-procurement portal)</td><td>13/10/2026 by 2:30 PM</td></tr>
<tr><td>8.</td><td>Date and Time of Opening of Technical Bids</td><td>14/10/2026 by 2:30 PM</td></tr>
<tr><td colspan="3">i. Eligibility Criteria: Please refer to Section 6 of the Tender Document.
ii. Two Bid System i.e. Stage-1 Prequalification cum Technical Bid; Stage-2 Commercial Bid.
iii. Tenders received after due date and time will be summarily rejected.
iv. Any Bid not conforming to the format will be summarily rejected.</td></tr>
</table>

Note: Bidders are advised to visit the e-procurement portal i.e. hptenders.gov.in of H.P Govt. on regular basis for updates/corrigendum issued by HPSEDC related to the tender.

SECTION 1

INSTRUCTIONS TO BIDDER ON ELECTRONIC TENDERING SYSTEM

1. Bidder should do Online Enrolment in this Portal using the option Click Here to Enroll available in the Home Page. Then the Digital Signature enrollment has to be done with the e-token, after logging into the portal. The e-token may be obtained from one of the authorized Certifying Authorities such as e-Mudhra CA/GNFC/IDRBT/MtnlTrustline/SafeScrpt/TCS.
2. Bidder then logs into the portal giving user id / password chosen during enrollment.
3. The e-token that is registered should be used by the bidder and should not be misused by others.
4. DSC once mapped to an account cannot be remapped to any other account. It can only be inactivated.
5. The Bidders can update well in advance, the documents such as certificates, purchase order details etc., under My Documents option and these can be selected as per tender requirements and then attached along with bid documents during bid submission. This will ensure lesser upload of bid documents.
6. After downloading / getting the tender schedules, the Bidder should go through them carefully and then submit the documents as per the tender document; otherwise, the bid will be rejected.
7. The BOQ template must not be modified/replaced by the bidder and the same should be uploaded after filling the relevant columns, else the bidder is liable to be rejected for that tender. Bidders are allowed to enter the Bidder Name and Values only.
8. If there are any clarifications, this may be obtained online through the eProcurement Portal, or through the contact details given in the tender document. Bidder should take into account of the corrigendum published before submitting the bids online.
9. Bidder, in advance, should prepare the bid documents to be submitted as indicated in the tender schedule and they should be in PDF/XLS/RAR/DWF formats. If there is more than one document, they can be clubbed together.
10. Bidder should arrange for the EMD as specified in the tender.
11. The bidder reads the terms and conditions and accepts the same to proceed further to submit the bids.
12. The bidder has to submit the tender document(s) online well in advance before the prescribed time to avoid any delay or problem during the bid submission process.
13. There is no limit on the size of the file uploaded at the server end. However, the upload is decided on the Memory available at the Client System as well as the Network bandwidth available at the client side at that point of time. In order to reduce the file size, bidders are suggested to scan the documents in 75-100 DPI so that the clarity is maintained and also the size of file also gets reduced. This will help in quick uploading even at very low bandwidth speeds.
14. It is important to note that, the bidder has to click on the Freeze Bid Button, to ensure that he/she completes the Bid Submission Process. Bids Which are not Frozen are considered as Incomplete/Invalid bids and are not considered for evaluation purposes
15. The Tender Inviting Authority (TIA) will not be held responsible for any sort of delay or the difficulties faced during the submission of bids online by the bidders due to local issues.
16. The bidder may submit the bid documents online-mode only, through this portal. Offline documents will not be handled through this system.
17. At the time of freezing the bid, the eProcurement system will give a successful bid Updation message after uploading all the bid documents submitted and then a bid summary will be shown with the bid no, date & time of submission of the bid with all other relevant details. The documents submitted by the bidders will be digitally signed using the e-token of the bidder and then submitted.
18. After the bid submission, the bid summary has to be printed and kept as an acknowledgement as a token of the submission of the bid. The bid summary will act as proof of bid submission for a tender floated and will also act as an entry point to participate in the bid opening event.
19. Successful bid submission from the system means, the bids as uploaded by the bidder is received and stored in the system. System does not certify for its correctness.
20. The bidder should see that the bid documents submitted should be free from virus and if the documents cannot be opened, due to virus, during tender opening, the bid is liable to be rejected
21. The time that is displayed from the server clock at the top of the tender Portal, will be valid for all actions of requesting bid submission, bid opening etc., in the e-Procurement portal. The Time followed in this portal is as per Indian Standard Time (IST), which is GMT+5:30. The bidders should

adhere to this time during bid submission.

22. All the data being entered by the bidders would be encrypted at the client end, and the software uses PKI encryption techniques to ensure the secrecy of the data. The data entered will not be viewable by unauthorized people during bid submission and not viewable by any one until the time of bid opening. Overall, the submitted bid documents become readable only after the tender opening by the authorized individual.
23. During transmission of bid document, the confidentiality of the bids is maintained since the data is transferred over secured Socket Layer (SSL) with 256-bit encryption technology. Data encryption of sensitive fields is also done.
24. The bidders are requested to submit the bids through online eProcurement system to the TIA well before the bid submission end date and time (as per Server System Clock).
25. The bidders are requested to submit the bids through online eProcurement system to the TIA well before the bid submission end date and time **(as per Server System Clock)**.

SECTION 2

1. INVITATION TO BID

Himachal Pradesh State Electronics Development Corporation Limited (HPSEDC) invites Bids from reputed, qualified, and experienced entities (including companies, LLPs, firms and MSMEs) for the establishment of a multi-agency Rate Contract of Empanelment of Agencies to provide end to end DPDP Compliance Services on behalf of various Govt. Departments/Organizations.

The Rate Contract, once established, shall be a non-exclusive arrangement. Empanel agencies shall publish their rates for each service package. All H.P Government Departments, Boards, Corporations, Autonomous Bodies, Local Bodies, Public Sector Undertakings, and Urban Local Bodies may draw on the Rate Contract to directly procure DPDP compliance services without initiating a fresh tender.

NOTE: Departments/HPSEDC may select individual services or bundles from empaneled agencies at their discretion.

2. BACKGROUND AND CONTEXT

2.1 The Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 (No. 22 of 2023), enacted on 11 August 2023 and notified under the Gazette of India, is India's landmark legislation governing the processing of digital personal data. The Act establishes rights for Data Principals (citizens) and obligations for Data Fiduciaries (organizations that determine purpose and means of processing).

Key provisions of the Act that create compliance obligations for Government Departments include:

i. **Consent Requirements** (Sections 5 & 6): Notices must be served in clear language; consent must be free, specific, informed, and revocable.

ii. **Data Fiduciary Obligations** (Section 8): Data Fiduciaries must implement security safeguards, notify breaches, and erase data upon fulfilment of purpose.

iii. **Children's Data** (Section 9): Verifiable parental/guardian consent is mandatory before processing personal data of children under 18 years.

iv. **Significant Data Fiduciary** (Section 10): Entities designated as SDFs by central government must appoint a DPO, conduct Data Protection Impact Assessments, and undertake periodic audits. The departments may also voluntarily adopt equivalent SDF-readiness controls before the central govt. notification.

v. **Rights of Data Principals** (Sections 11-14): Rights to access, correct, erase, and nominate, along with grievance redressal mechanisms.

vi. **Cross-border Transfer Restrictions** (Section 16): Data transfer to certain jurisdictions may be restricted by Central Government notification.

vii. **Penalties (Schedule)**: Fines up to Rs. 250 Crore for breach of security safeguards; Rs. 200 Crore for failure to notify breaches; Up to Rs. 50 Crore Non-compliance with Data Principal Rights; Up to 150 Crore Failure to comply with duties of Significant Data Fiduciary.

2.2 The DPDP Rules, 2025

The Digital Personal Data Protection Rules, 2025 (published 13 November 2025) operationalize the Act.

Rules 3 to 16: create detailed procedural requirements around notice formats, security safeguards (including encryption, masking, logging, access controls and 72-hour breach notification to the Board), data retention timelines and rights of Data Principals.

Rules 17 to 23: establish the Data Protection Board structure. These Rules are now in force on a phased basis, with the bulk of obligations commencing 18 months from publication.

2.3 Compliance Imperative for H.P Government

The Government of H.P. operates various citizen-facing digital services involving significant data processing activities. Departments will be required to maintain readiness to comply with applicable DPDP requirements upon issuance of relevant Government notifications and directions. Failure to comply may result in regulatory, financial and reputational risks, including erosion of citizen trust.

HPSEDC intends to facilitate state-wide DPDP compliance through establishment of this Rate Contract enabling every department to access qualified experts without the burden of individual procurement.

3. OBJECTIVES OF THIS RFP

HPSEDC seeks to achieve the following objectives through this procurement: -

a) Establish a pre-qualified pool of agencies capable of delivering end-to-end DPDP Act compliance services across all Government of H.P entities.

b) Create a published Rate Contract with transparent, pre-negotiated rates for each service line — enabling departments to engage quickly without independent tendering.

c) Drive state-wide DPDP compliance uniformly by lowering the procurement and procurement capacity barrier for smaller departments, boards, and local bodies.

d) Ensure quality assurance through defined SLAs, performance security, and periodic review mechanisms embedded in the Rate Contract.

NOTE: Empaneled agencies will NOT receive guaranteed volumes. Each department will independently place work orders. Agencies must be prepared to commence services within timelines specified herein upon receipt of a valid work order referencing this Rate Contract.

4. RATE CONTRACT FRAMEWORK

4.1 Nature of the Rate Contract

The Rate Contract established pursuant to this RFP shall operate as follows:

a) HPSEDC shall empanel technical and commercial qualifying agencies.

b) Each empanel agency should publish a Rate Card (per Annexure D) for all the service lines.

c) Any GOHP entity may, upon receipt of administrative approval, issue a Work Order through HPSEDC to any empaneled agency citing this Rate Contract reference.

d) Consortium bidding is not permitted under this tender. However, the bidder may submit supporting documents, CVs, Certifications, Work orders from its OEMS, along with the duly authorized MAF, as evidence of eligibility for the service lines.

e) The total duration of empanelment shall be valid for 3 years and further may be extended subject to administrative approval by HPSEDC.

f) **Bidder/Empaneled Agency Responsibility:** The empaneled agency shall be solely responsible for meeting the required eligibility, service delivery, qualified personnel, implementation and support obligations under the Rate Contract and respective Work Orders.

4.2 Rate Contract Hierarchy

Level	Actor	Action
L1	HPSEDC	Establishes Rate Contract; sets ceiling rates; manages empanelment
L2	GOH.P Department / Entity	Issues Work Order to empaneled agency through HPSEDC, citing Rate Contract number
L3	Empaneled Agency	Delivers services; invoices department; reports to HPSEDC quarterly
L4	HPSEDC (oversight)	Monitors SLA compliance; reviews agency performance; handles escalations

4.3 Service line Mechanism

Agencies offering all service lines shall be eligible for empanelment. The rate card submitted by the agencies must clearly specify service-wise pricing. State Government Departments/Organizations may avail itself of any single or all these services through HPSEDC from the empaneled agencies for compliance with the provisions of the DPDP Act.

5. SCOPE OF WORK

This section defines the detailed deliverables, timelines, and outputs required for each of the service lines. A single agency must offer all the service lines.

5.1 Service Line 1: DPDP Gap Assessment & Audit

Attribute	Details
Service Code	SL-01
Primary Beneficiary	All GOH.P Departments / Entities designated as Data Fiduciaries
Trigger	Work Order by Department; or as mandated by GOH.P IT Dept. Circular
Completion Timeline	Within 8 weeks of Work Order date

Scope & Deliverables

a) **Data Mapping & Inventory:** Comprehensive identification and documentation of all personal data flows (collection, storage, processing, sharing, and disposal) across the department's digital and physical systems. Produce a Data Flow Register in prescribed format.
b) **Legal Basis Assessment:** Evaluate each processing activity against DPDP Act Sections 4, 5, 6, and 7. Classify each activity as: Consent-based, Legitimate Use or Non-compliant. Provide a Processing Register.
c) **Security Controls Assessment:** Assess technical controls against Rule 6 requirements — encryption at rest and in transit, access controls, logging, monitoring, and backup mechanisms.
d) **Children's Data Review:** Identify any process involving data of minors; assess compliance with Section 9 and Rule 10 (verifiable parental consent requirements).
e) **Third Party & Data Processor Review:** Map all data processors; assess whether contracts contain prescribed security provisions per Rule 6(1)(f).
f) **Cross-Border Transfer Assessment:** Identify any personal data transferred outside India; assess compliance with Section 16.
g) **Gap Report:** Detailed gap analysis document with risk rating (Critical / High / Medium / Low) for each gap, mapped to specific Act/Rule provisions.
h) **Remediation Roadmap:** Prioritized action plan with timelines, responsibilities, and estimated effort for each remediation item.
i) **Executive Summary Report:** Board/Secretary-level summary (max. 10 pages) suitable for presentation to Department head.
j) **Annual Compliance Audit (Repeat):** For departments designating Significant Data Fiduciaries (SDFs), an annual re-audit to assess progress and issue updated compliance posture report.

5.2 Service Line 2: Data Protection Officer (DPO) as-a-Service

Attribute	Details
Service Code	SL-02
Applicable Entities	Significant Data Fiduciaries (SDFs) under Section 10; other departments by choice
Engagement Model	Retainer-based; dedicated or shared DPO depending on department size
Minimum Qualification of DPO	LLB + 5 years of data privacy experience + CIPP/CIPM/CDPSE/BCI certified. Sound working knowledge of Hindi.
Availability	Minimum 8 hrs./week dedicated to department; escalation response within 4 hours

Scope & Deliverables

a) Legal Representation: Act as the department's designated DPO as required under Section 10(2)(a); represent the department before the Data Protection Board of India (DPBI) in all proceedings.
b) Where the appointing entity is formally designated as an SDF, the service shall provide an eligible individual DPO based in India and responsible to the competent governing body, in accordance with Section 10(2)(a) of the DPDP Act.
c) Policy Development: Draft, review, and maintain: Privacy Policy; Consent Notice templates (multilingual, including Hindi per Section 5(3)); Data Retention Policy; Data Subject Rights Procedure; Vendor Data Processing Agreements.

d) DPIA Management: Conduct periodic Data Protection Impact Assessments as mandated under Section 10(2)(c) and Rule 13. Maintain DPIA register.
e) Regulatory Monitoring: Monitor amendments to the DPDP Act, Rules, DPBI regulations, and MeitY notifications. Issue monthly regulatory update notes to the department.
f) DSAR Handling: Manage and respond to Data Subject Access Requests (Sections 11, 12, 13 of the Act) within prescribed timelines. Maintain DSAR log.
g) Grievance Redressal Oversight: Oversee the department's grievance mechanism under Section 8(10); ensure response within 90-day limit per Rule 14(3).
h) Board Liaison: Act as the single point of contact for DPBI communications, notices, and show-cause proceedings.
i) Monthly Compliance Report: 2-page monthly status report submitted to department head and HPSEDC portal.
j) Annual DPIA Report: Formal annual DPIA report filed with the DPBI per Rule 13(2).

5.3 Service Line 3: Consent Management Platform (CMP)

Attribute	Details
Service Code	SL-03
Deployment Model	SaaS (preferred); on-premise on department request
Integration Requirement	Must integrate with APIs, SSO, and State Data Centre (SDC)
Data Residency	All data must reside within India; preference for NDC/SDC hosting
Language Support	Hindi + English mandatory
Implementation Timeline	Go-live within 12 weeks of Work Order

Functional Requirements

a) Consent Collection: Granular, purpose-specific consent capture per Sections 5 & 6 — free, informed, specific, unambiguous.
b) Consent Withdrawal: One-click withdrawal mechanism with ease comparable to grant (Section 6(4)).
c) Multi-language Notice Delivery: Serve consent notices in any of the 22 Eighth Schedule languages (Hindi + English).
d) Consent Audit Trail: Immutable, timestamped log of all consent events (grant, withdrawal, update) minimum 7-year retention per Schedule I-B of Rules.
e) Consent Manager Interoperability: Platform must be able to onboard or integrate with registered Consent Managers as per Section 6(7) and Rule 4 when the DPBI notifies them.
f) Parental Consent Workflow: Verifiable parental/guardian consent workflow for children's data per Rule 10, including Aadhaar/Digi Locker integration for age verification.
g) DSAR Portal: Citizen-facing portal for submission of data access, correction, erasure, and nomination requests per Sections 11-14.
h) Dashboard & Analytics: Real-time dashboard showing consent rates, withdrawal rates, DSAR volumes, and SLA compliance — accessible to department DPO.
i) API Integration: RESTful APIs for integration with department citizen portals, apps, and backend systems.

Note: Withdrawal of consent shall not require cessation or erasure where continued processing or retention is required or authorised under applicable law. In such cases, the applicable lawful basis, justification and retention period shall be recorded, and only the processing necessary for such purpose shall continue.

Technical & Security Requirements

a) ISO 27001 certified infrastructure.
b) End-to-end encryption (AES-256 at rest; TLS 1.3 in transit).
c) Role-based access control (RBAC) with audit logs.
d) MeitY empaneled cloud provider (preferred) or NIC cloud.
e) 99.5% uptime SLA; RTO 4 hours; RPO 1 hour.

5.4 Service Line 4: Data Discovery & Classification Tool

Attribute	Details
Service Code	SL-04
Deployment Model	SAAS (Preferred)/On premises / Private Cloud / Hybrid; no personal data to leave department’s boundary
Scan Targets	Databases (On-Premises & Cloud), Email, Collaborations tools, Enterprise Chat, SAAS Applications, NFS, DMS, AI Platform.
Classification Framework	Aligned to DPDP Act: Personal Data / Children's Data / Cross-border Flagged
Implementation Timeline	Tool deployed and first scan completed within 5 weeks of Work Order

Scope & Deliverables

a. Purpose of the Solution
The Data Discovery and Classification solution provides organizations with continuous visibility, understanding, and control over digital personal data across the enterprise.
Its primary purpose is to enable organizations (Data Fiduciaries) to:

- Identify what personal data they hold
- Understand where it resides
- Classify it based on sensitivity, context, and regulatory obligations
- Link personal data to consent, purpose, and retention
- Enforce DPDP Act requirements across data lifecycles

b. Regulatory Context – Role in DPDP Act Compliance
The DPDP Act requires Data Fiduciaries to:

- Process personal data only for lawful and specified purposes
- Maintain visibility into personal data processed digitally
- Enable access, correction, erasure, and grievance redressal
- Honour consent withdrawal
- Delete data once the purpose is fulfilled
- Demonstrate compliance to the Data Protection Board when required

c. Scope of Coverage
c.1 Data Types

- Digital personal data (native digital or digitized)
- Employee data, customer data, partner data
- Children's personal data
- Business data containing embedded personal data

c.2 Data Environments

- Structured data: databases, data warehouses, applications
- Unstructured data: file shares, collaboration tools, email, endpoints
- Cloud infrastructure and SaaS platforms
- Backup, archive, and data lake environments

c.3 Functional Architecture Overview
The solution consists of the following logical components:

- Data Discovery Engine
- Content Inspection & Classification Engine
- Metadata & Personal Data Inventory
- Consent Integration & Mapping Layer
- Policy & Purpose Enforcement Engine
- Rights Fulfilment Enablement Layer
- Reporting, Audit & Compliance Interface
- Security, Governance & Controls

d. Data Discovery – Functional Requirements
d.1 Automated Enterprise-Wide Discovery
The solution shall automatically discover data across:

- On-premises and cloud data stores
- Structured and unstructured repositories
- SaaS and business applications
- AI Platform & Collaboration platforms

Discovery must support:

- Agent-based and Agentless mechanisms
- Scheduled and continuous scanning
- Incremental discovery of new or modified data

d.2 Identification of Digital Personal Data
The solution must identify:

- Direct identifiers (name, email, phone number)
- Government-issued identifiers (where present)
- Financial, health, employment, and demographic attributes
- Contextual identifiers that make individuals identifiable

Discovery must work across formats, languages, and semi-structured content.
d.3 Data Principal Correlation
The solution shall:

- Correlate data elements belonging to the same Data Principal
- Maintain a consolidated view of a Data Principal's data footprint
- Track data copies and derivatives across systems

e. Data Classification – Functional Requirements

e.1 Classification Model

The solution shall classify data across multiple dimensions:

Regulatory Classification

- Personal Data
- Children's Personal Data
- Employee Personal Data
- High-risk personal data (contextual)

Operational Classification

- Sensitivity level
- Business criticality
- Exposure risk

e.2 Classification Techniques

- Pattern-based classification (rules and policies)
- Context-aware classification (source, system, user)
- Machine-assisted content analysis
- Manual validation and override with audit trail

e.3 Dynamic & Continuous Classification

- Re-classification when data content or context changes
- Automatic updates based on consent or purpose changes
- Support for real-time enforcement scenarios

f. Consent Management Integration (Core Requirement)

f.1 Bidirectional Integration

The solution must integrate with a Consent Management platform to:

- Consume consent status, purpose, and validity
- Associate consent metadata with classified data entities
- Update consent status in near real time

f.2 Consent-Aware Data Mapping

Each personal data element must be mapped to:

- Consent identifier
- Declared purpose of processing
- Consent state (active, withdrawn, expired)
- Applicable retention period

f.3 Consent Enforcement

The solution shall:

- Flag or restrict processing when consent is withdrawn
- Trigger deletion, anonymization, or quarantine workflows
- Support legitimate-use exceptions where legally applicable

f.4 Self-Service Access Requests and Entitlement Reviews

To reduce IT overhead while maintaining security discipline, the solution shall support delegated access governance workflows:

- End users shall be provided with an intuitive web interface through which they can request access to specific data resources, applications, and security groups, with requests routed directly to identified data owners for approval.
- Data owners, who possess the operational context to make informed access decisions, shall be empowered to grant time-bound or permanent access without requiring IT intervention for routine requests.
- Periodic entitlement reviews shall be scheduled automatically based on organizational policy, prompting data owners and line managers to certify or revoke existing access grants.
- Users identified as no longer requiring access — due to role change, project completion, or departure — shall be automatically flagged for access removal, with owners notified for confirmation.
- Just-in-time access provisioning shall be supported for privileged scenarios, granting elevated access for a defined window before automatic revocation.

f.5 Retention Management and Storage Optimization

- The solution shall enforce granular retention schedules derived from applicable legal obligations under the DPDP Act and departmental data management policies.
- Data that has exceeded its mandated retention period shall be automatically identified and queued for review, archival, or secure deletion, subject to the applicable approval workflow.
- Stale data — files and records that have not been accessed within a configurable threshold period — shall be automatically transferred to a designated secure archival location, optimizing primary storage utilization and reducing the active attack surface for data breaches.
- Storage consolidation policies shall enable administrators to identify and remove duplicate or redundant copies of personal data, reducing unnecessary data proliferation and compliance exposure.

g. Purpose Limitation & Retention Controls

g.1 Purpose Binding

- Every dataset must be tagged with its processing purpose
- Alerts must be generated for purpose deviation
- Purpose reuse must be explicitly authorized

g.2 Retention Lifecycle Management

- Retention policies linked to purpose and consent
- Automated expiry tracking
- Secure deletion or anonymization workflows

h. Data Principal Rights Enablement

The solution shall enable:

- Rapid discovery of all data tied to a Data Principal
- Automated workflows for access, correction, and erasure
- Evidence generation for request fulfilment timelines

i. Breach Impact Assessment Support

In the event of a personal data breach, the solution must:

- Identify affected Data Principals
- Assess volume and sensitivity of impacted data
- Support breach notification decision-making

j. Reporting, Audit & Compliance

j.1 Compliance Visibility

Dashboards and reports covering:

- Personal data inventory
- Consent coverage gaps
- High-risk data repositories
- Children's data processing

j.2 Audit & Evidence Readiness

- Tamper-proof audit logs
- Regulator-ready compliance reports
- Inputs for DPIAs and Significant Data Fiduciary obligations

k. Security & Governance Controls

- Role-based access controls (RBAC)
- Least-privilege enforcement
- Encryption of metadata and classifications
- Integration with enterprise security tools

5.5 Service Line 5: Personal Data Access Assurance Tool

Attribute	Details
Service Code	SL-05
Deployment Model	SAAS (Preferred)/On-premises / Private Cloud / Hybrid; no personal data to leave department's boundary
Scan Targets	Active Directory/LDAP/Entra AD
Classification Framework	Aligned to DPDP Act: Personal Data / Children's Data / Cross-border Flagged
Implementation Timeline	Tool deployed and first scan completed within 5 weeks of Work Order

Scope & Deliverables

a. Purpose of the solution

The Personal Data Access Assurance solution provides continuous monitoring, analysis, and control of user and service identities that access digital personal data.
Its purpose is to:

- Prevent unauthorized processing of personal data
- Detect identity-based attacks before data exfiltration occurs
- Enforce least privilege and purpose-bound access
- Provide evidence of "reasonable security safeguards" as mandated by DPDP Act Section 8(5)

This solution operates **in conjunction with Data Discovery & Classification** to shift security from **perimeter-based** to **data-centric identity enforcement**.

b. Regulatory Context – Why Personal Data Access Assurance Is Mandatory for DPDP

Under the DPDP Act:

- Unauthorized access itself constitutes a personal data breach
- Data Fiduciaries must implement technical safeguards to prevent misuse

- Organizations must demonstrate accountability and auditability
- Breach penalties can reach **₹250 crore**, especially where access controls fail

c. Scope of Identity Coverage

c.1 Identities Covered

- Human users (employees, contractors, partners)
- Privileged administrators
- Service accounts and application identities
- API and automation identities

c.2 Access Surfaces Monitored

- File systems and collaboration platforms
- Databases and data platforms
- Cloud services and SaaS applications
- Endpoints and remote access sessions

d. Core Functional Components

1. Identity Activity Monitoring Engine
2. Behavioral Analytics & Baseline Engine
3. Privilege & Entitlement Risk Engine
4. Data-Aware Access Correlation Layer
5. Threat Detection & Response Engine
6. Audit, Forensics & Compliance Interface

e. Identity Activity Monitoring

e.1 Continuous Identity Telemetry

The solution shall continuously monitor:

- Authentication events
- File and data access actions
- Permission changes
- Privileged operations
- Lateral movement attempts

Telemetry must be collected in near real-time across on-premises, cloud, and SaaS environments.

f. Behavior-Based Identity Analytics

f.1 Normal Behavior Baselines

The solution shall:

- Establish behavioral baselines per identity
- Learn typical access patterns, volumes, and timing
- Adapt baselines dynamically as roles evolve

f.2 Anomaly Detection

Detect deviations such as:

- Sudden access to large volumes of personal data
- Access to data outside business role or purpose
- Unusual access times or locations
- Rare or first-time access to sensitive datasets

g. Privilege & Entitlement Risk Management

g.1 Least-Privilege Enforcement

The solution must:

- Identify excessive, unused, or risky permissions
- Continuously assess access against actual usage
- Highlight identities with unnecessary access to personal data

g.2 Privileged Identity Monitoring

- Track administrator and elevated account activity
- Detect misuse of high-risk privileges
- Correlating privileged actions with data sensitivity

h. Integration with Data Discovery & Classification

h.1 Data-Aware Identity Context

The Personal Data Access Assurance Solution shall ingest:

- Data sensitivity classifications
- Personal data indicators
- Children’s data and high-risk categories
- Consent and purpose metadata (indirectly via data layer)

h.2 Joint Risk Scoring

Risk scoring must combine:

- Identity behavior anomalies
- Permission exposure
- Data sensitivity of accessed assets

i. Integrated Use Cases – Early Detection & Threat Blocking

Use Case 1: Compromised User Account

- Identity suddenly accesses large volumes of classified personal data
- Data Discovery confirms sensitivity and consent scope
- Personal Data Access Assurance Solution flags abnormal behavior
- Automated response: suspend access, alert security

Use Case 2: Insider Data Misuse

- Legitimate user accesses personal data outside assigned purpose
- Data classification indicates high-risk category
- Behavior deviates from historical baseline
- Incident flagged before mass extraction

Use Case 3: Privileged Account Abuse

- Admin account accesses unstructured repositories containing personal data
- Personal Data Access Assurance Solution detects rare behavior
- Data layer confirms presence of regulated data
- Immediate containment initiated

Use Case 4: Consent Withdrawal Enforcement

- Consent withdrawn via Consent Manager
- Data remains present but access should cease
- Identity attempts to access withdrawn-consent data
- Access blocked and logged

j. Automated Response & Threat Blocking

The solution shall support:

- Session termination
- Account suspension
- Access throttling
- Just-in-time access revocation
- Integration with SOC/SIEM workflows

k. Audit, Forensics & Compliance Evidence

The solution must provide:

- Immutable identity activity logs
- Clear timelines for investigations
- Proof of access control enforcement
- Regulator-ready incident evidence

5.6 Service Line 6: Training & Awareness Program

Attribute	Details
Service Code	SL-05
Target Audience	GOH.P Officers (IAS/HAS/HPS), Departmental Staff, IT Teams, DPOs, C-Suite
Mode	In-person workshops; live virtual sessions; self-paced e-Learning (LMS)
Medium	Hindi + English; all materials bilingual
Certification	Completion certificates; linked to DPDP compliance records

Training Modules (Minimum)

#	Module	Target Audience	Duration	Mode
M1	DPDP Act Essentials	All GOH.P Staff	1.5 hrs	e-Learn
M2	DPO Foundation Programme	Designated DPOs	9 hrs	In-person
M3	Senior Leadership Awareness	Secretaries / HoDs	2 hrs	Workshop
M4	IT & Security Team Deep-Dive	IT Officers / CISOs / SOC Team	8 hrs	Workshop
M5	Consent & Notice Handling	Front-line / Citizen Services Staff / IT Teams	1 hrs	e-Learn
M6	Breach Response Drill	IT + Legal + Comms Teams + SOC	6 hrs	Simulation
M7	Annual Refresher	All Certified Staff	2 hrs	e-Learn

Additional Deliverables

a) LMS Deployment: Host all e-learning modules on a SCORM-compliant LMS integrable with NIC e-Sampark or GOH.P HR systems.

b) Phishing / Social Engineering Simulation: Minimum 2 simulated campaigns per year to assess staff awareness.

c) Training Effectiveness Report: Pre- and post-test scores; completion rates; department-wise compliance dashboard.
d) Content Ownership: All training materials, IP, and LMS content shall vest with GOH.P upon contract expiry.

5.7 Service Line 7: Breach Response & Notification Service

Attribute	Details
Service Code	SL-07
Availability	24x7x365 Incident Response Hotline
Initial Response SLA	Acknowledge within 1 hour; Preliminary Assessment within 4 Hours
Mandatory Legal Timeline	Rule 7(2): Board notification within 72 hours; Data Principal notification without delay
Retainer Model	Annual retainer fee (as per Rate Card, Annexure D)

Scope & Deliverables

a) Breach Retainer & Readiness: Maintain a Breach Response Plan (BRP) for each subscribed department. Conduct bi-annual tabletop exercises to test readiness.
b) Incident Detection Support: 24x7 monitoring integration with department SIEM/SOC; alert triaging; false positive management.
c) Containment & Forensics: On-site or remote forensic investigation; containment measures; root-cause analysis; evidence preservation chain of custody.
d) Impact Assessment: Quantify nature, extent, and affected Data Principals per Rule 7(2)(a). Classify breach severity.
e) Board Notification: An intimation without delay, followed by draft and submit initial notification to DPBI within 72 hours per Rule 7(2)(b). Submit follow-up detailed report including events, reasons, remediation, and Data Principal notification status.
f) Data Principal Notification: Draft clear, plain-language notifications to affected individuals per Rule 7(1). Manage bulk notification via email, SMS, and in-app channels.
g) Regulatory Liaison: Manage all DPBI communications, information requests (Rule 23), and show-cause responses on behalf of the department.
h) Post-Breach Review: Publish a Post-Incident Review (PIR) report within 30 days; update Breach Response Plan; recommend technical and process changes.
i) Evidence Package: Compile complete documentation package for DPBI inquiry compliance per Sections 27-28 of the Act.
j) Media & Communications Advisory: If breach attracts media attention, provide communications advisory and draft public statements.

5.8 Service Line 8: Data Loss Prevention Solution

Attribute	Details
Service Code	SL-08
Deployment Model	SAAS / On premises / Private Cloud / Hybrid; no personal data to leave department's boundary
Scan Targets	Endpoints/ Network / Email / DB Hardening
Classification Framework	Aligned to DPDP Act: Personal Data / Children's Data / Cross-border Flagged
Implementation Timeline	Tool deployed and first scan completed within 5 weeks of Work Order

Scope & Deliverables

a. Purpose of the Data Loss Prevention Solution
The Data Loss Prevention (DLP) solution is designed to prevent unauthorized disclosure, transmission, or exfiltration of digital personal data, whether caused by:

- External cyberattacks
- Compromised identities
- Insider misuse (intentional or accidental)
- Misconfigured systems or processes

Under the DPDP Act, unauthorized access or disclosure constitutes a personal data breach, attracting regulatory penalties and breach-notification obligations.
The DLP solution acts as a last-mile enforcement layer, ensuring personal data cannot leave authorized boundaries, even if other controls fail.

b. Regulatory Context – Why DLP Is Mandatory for DPDP Compliance
The DPDP Act and Rules explicitly require Data Fiduciaries to implement:

- Reasonable security safeguards
- Controls to prevent unauthorized access or disclosure

- Continuous monitoring and logging
- Timely breach detection and containment

Rule 6 of the DPDP Rules, 2025 places specific emphasis on:

- Access monitoring
- Detection of unauthorized activity
- Controls that reduce the usability of infiltrated data

A DLP solution is therefore a core compliance control, not an optional security add-on.

c. Scope of Protection

c.1 Data in Scope

- Personal data
- Children's personal data
- Employee and customer data
- High-risk and sensitive personal data (contextual)
- Data subject to consent or purpose limitations

c.2 Channels in Scope

- Email (inbound, outbound, internal)
- File transfers and uploads (Data Transfer modes)
- Web and cloud apps
- Endpoints (copy, print, USB)
- Cloud storage sharing
- API-based data movement
- Databases

d. Core Functional Components

1. Data-Aware Policy Engine
2. Channel Monitoring & Inspection Layer
3. Real-Time Enforcement Engine
4. Incident Detection & Escalation Engine
5. Forensic Logging & Compliance Reporting

e. Deep Integration with Data Discovery & Classification

e.1 Data-Driven Policy Creation (Mandatory)

The DLP solution must not rely on static patterns alone. It shall ingest outputs from the Data Discovery & Classification solution, including:

- Data sensitivity labels
- Personal data identifiers
- Contextual risk scores
- Children's data and special categories
- Retention and purpose metadata

e.2 Classification-Aware DLP Decisions

All DLP enforcement decisions must evaluate:

- What data is being moved
- Its classification and sensitivity
- Applicable consent and purpose
- Risk level of the destination channel

f. Channel-Specific DLP Controls

f.1 Email DLP

- Inspect body and attachments before delivery
- Block, quarantine, or encrypt emails containing classified personal data
- Prevent auto-forwarding of personal data to unauthorized domains

f.2 Endpoint DLP

- Prevent copying personal data to USB or removable media
- Control screen capture, printing, and clipboard actions
- Detect bulk file staging activity prior to exfiltration

f.3 Cloud & SaaS DLP

- Monitor uploads and shares in cloud storage
- Block public or external sharing of classified data
- Detect abnormal download or sync activity

f.4 Web & API DLP

- Inspect uploads to external websites or APIs
- Prevent data submission to unauthorized services
- Apply real-time controls on unsanctioned cloud usage

g. Early Detection & Threat Blocking – Integrated Use Cases

Use Case 1: Compromised Account Data Exfiltration

- Data Discovery tags files as high-risk personal data
- Account suddenly initiates bulk uploads externally
- DLP detects risky transfer based on classification
- Upload blocked before data leaves organization

Use Case 2: Insider Accidental Data Leakage

- Employee emails spreadsheet with personal data to incorrect recipient
- DLP identifies classified content in attachment
- Email quarantined and security alerted

Use Case 3: Malicious Insider Behaviour

- User stages data locally and attempts mass extraction
- Data classification confirms regulated personal data
- DLP detects volume anomaly and blocks transfer

Use Case 4: Consent Withdrawal Enforcement

- Consent withdrawn for specific personal data
- Data remains in systems but must not be shared
- DLP blocks attempted sharing post-withdrawal

h. Incident Escalation & Breach Readiness

h.1 Incident Classification

Each DLP event must be categorised as:

- Policy violation
- Security incident
- Potential personal data breach

h.2 Breach Impact Reduction

- Immediate containment prevents breach escalation
- Limits requirement for regulator and Data Principal notification

i. Audit, Evidence & Compliance Reporting

The solution must provide:

- Tamper-proof logs of blocked and allowed actions
- Clear mapping between data classification and enforcement
- Evidence of continuous monitoring
- Incident timelines and response records

j. Security & Governance Controls

- Role-based policy administration
- Separation of duties
- Policy change audit trails
- Integration with SOC and SIEM platforms

k. Compliance & Business Outcomes

When combined with Data Discovery & Classification, the DLP solution:

- Converts data visibility into enforced protection
- Enables early-stage attack detection
- Blocks threats before data exposure occurs
- Reduces regulatory, financial, and reputational risk
- Provides strong DPDP defensibility

l. Why DLP + Discovery Is Essential (Not Optional)

Without Integration	With Integration
Blind blocking	Risk-aware enforcement
High false positives	Precision-based decisions
Reactive breach response	Preventive compliance
Weak audit defence	Strong regulator evidence

5.9 Service Line 9: Personal Data Intelligent Processing Guard Solution:

Attribute	Details
Service Code	SL-09
Deployment Model	SAAS / On-premises / Private Cloud / Hybrid; no personal data to leave department's boundary
Scan Targets	OpenAI ChatGPT Enterprise, Microsoft Co-pilot, Hosted AI Platforms, Custom LLM and Agentic Framework, Embedded AI, Shadow AI, AI Development Tools.
Classification Framework	Aligned to DPDP Act: Personal Data / Children's Data / Cross-border Flagged
Implementation Timeline	Tool deployed and first scan completed within 5 weeks of Work Order

Scope & Deliverables

a. Purpose of the Personal Data Intelligent Processing Guard Solution

The Personal Data Intelligent Processing Guard solution is designed to secure the interaction between AI systems and digital personal data, ensuring that:

- Personal data is not misused, over-exposed, or exfiltrated through AI
- AI models and prompts do not violate consent, purpose limitation, or retention

- AI becomes an early indicator of compromise, not a new data-leak surface

Under the DPDP Act, AI systems that process, infer from, or generate outputs using personal data are treated as data fiduciary-controlled processing mechanisms, making them subject to the same safeguarding, breach, and accountability requirements as traditional systems.

b. Regulatory Context – Why Personal Data Intelligent Processing Guard Is Mandatory Under DPDP

The DPDP Act imposes:

- Consent-first processing
- Purpose limitation and data minimization
- Accountability for inferred and derived data
- Strong safeguards against unauthorized disclosure AI systems amplify DPDP risks by:
- Aggregating large volumes of personal data
- Inferring new personal attributes
- Enabling indirect data exfiltration through prompts, embeddings, and responses Regulators and advisory bodies explicitly identify AI as a **high-risk processing context** requiring stronger governance and technical safeguards.

c. Scope of Personal Data Intelligent Processing Guard Coverage

c.1 AI Systems in Scope

- Generative AI (text, code, image)
- Enterprise copilots and assistants
- ML models consuming organizational datasets
- Analytics and recommendation engines
- AI-powered automation and decision systems

c.2 Data Interactions Secured

- Training data ingestion
- Prompt and query inputs
- Model outputs and responses
- Embeddings and intermediate representations
- Data cached or reused across sessions

d. Core Functional Components

1. AI Data Awareness & Context Layer
2. Prompt & Interaction Inspection Engine
3. AI Output Risk Control Engine
4. Behavioral Anomaly Detection for AI Usage
5. Real-Time Response & Blocking Engine
6. AI Activity Audit & Compliance Interface

e. Deep Integration with Data Discovery & Classification

e.1 Classification-Driven AI Awareness

The Personal Data Intelligent Processing Guard solution must ingest and rely on outputs from the Data Discovery & Classification solution, including:

- Location of personal and sensitive data
- Data classification labels and risk scores
- Children's data indicators
- Retention and purpose metadata

This ensures AI interactions are evaluated based on actual data sensitivity, not generic rules.

e.2 AI Contextual Guardrails

AI interactions must be dynamically constrained based on:

- Whether the data requested exists
- Its classification and consent scope
- Whether it is permitted for use in AI processing

f. Prompt & Input Security Controls

f.1 Prompt Inspection

The solution shall inspect AI prompts to:

- Detect attempts to retrieve classified personal data
- Identify mass-extraction or enumeration patterns
- Detect prompt manipulation designed to bypass controls

f.2 Consent & Purpose Validation

Before AI processing:

- Validate that requested data aligns with declared purpose
- Block prompts involving withdrawn or expired consent
- Restrict processing of children's personal data

g. AI Output Security Controls

g.1 Output Classification

All AI responses must be:

- Analyzed for presence of personal or sensitive data
- Evaluated against classification metadata
- Scored for regulatory and business risk

g.2 Output Enforcement
Based on risk:

- Mask or redact sensitive content
- Block output entirely
- Require secondary authorization
- Log for investigation and review

h. Behavioral AI Anomaly Detection
h.1 Normal AI Usage Baselines
The solution shall establish:

- Typical AI query volumes per identity or role
- Normal data domains accessed via AI
- Time-based and behavioral patterns

h.2 Detection of AI-Driven Attacks
Detect scenarios such as:

- Sudden spike in AI queries involving personal data
- Repeated attempts to infer or reconstruct identities
- Lateral movement using AI to explore data context

i. Integrated Use Cases – Early Detection & Threat Blocking
Use Case 1: AI-Assisted Data Exfiltration Attempt

- Data Discovery identifies high-risk personal data
- User prompts AI to summaries or extract that data
- Personal Data Intelligent Processing Guard detects classification mismatch
- Output blocked before data disclosure

Use Case 2: Compromised Identity Using AI for Reconnaissance

- Attackers use AI assistant to explore datasets
- Behavior deviates from normal usage Personal Data Intelligent Processing Guard flags anomaly
- Security alerted before large-scale access begins

Use Case 3: Consent Withdrawal Enforcement in AI

- Consent withdrawn for a dataset
- AI prompt attempts access based on prior availability
- Personal Data Intelligent Processing Guard denies response and logs event

Use Case 4: Insider Misuse via AI Queries

- Legitimate user attempts to infer sensitive attributes
- Data classification indicates restricted category
- Personal Data Intelligent Processing Guard blocks inference-based leakage

j. Real-Time Response & Blocking
The solution shall support:

- Immediate response blocking
- Adaptive guardrail tightening under attack
- Integration with SOC and incident workflows
- Progressive enforcement (warn → restrict → suspend)

k. Audit, Accountability & Compliance Evidence
The solution must provide:

- Complete AI interaction logs
- Input/output traceability
- Proof of preventive controls
- Regulator-ready compliance reporting

5.10 Service Line 10: Database Activity Monitoring Solution

Attribute	Details
Service Code	SL-10
Deployment Model	SAAS / On-premise / Private Cloud / Hybrid; no personal data to leave department's boundary
Scan Targets	MSSQL, MySQL, Oracle, PostgreSQL, Snowflake, Databricks, AWS RDS, Azure DB, GCP Cloud SQL, Mongo DB
Classification Framework	Aligned to DPDP Act: Personal Data / Children's Data / Cross-border Flagged
Implementation Timeline	Tool deployed and first scan completed within 5 weeks of Work Order

Scope & Deliverables

a. Purpose & DPDP Compliance Role
a.1 Purpose
The DAM solution shall provide continuous, near real-time visibility into all database activity across in-scope environments, including:

- Human user activity (DBAs, analysts, developers)
- Application/service account activity
- Privileged operations and configuration changes
- Access to sensitive tables/columns and high-risk datasets

a.2 Why DAM is essential for DPDP

DPDP compliance requires reasonable security safeguards, including access controls, monitoring/logging, and detection of unauthorized access, and the ability to investigate and evidence compliance.

DAM operationalizes this by:

- Detecting unauthorized processing (read/write/export)
- Maintaining audit trails for who accessed what and when
- Supporting rapid breach triage (scope, impacted datasets, suspected identities)

b. Scope & Supported Database Targets (Functional)

b.1 Minimum database coverage (should support)

The solution should monitor common enterprise databases and platforms, at minimum including:

- Oracle, Microsoft SQL Server, MySQL (minimum baseline)
- Linux and Windows hosted databases
- On-prem, Cloud and virtual environments

b.2 Access paths to monitor

The solution shall capture database activity regardless of access method:

- Local and remote database access
- ODBC/JDBC initiated sessions
- CLI tools, admin consoles, and application middleware connections

c. Core Architecture & Deployment Capabilities

c.1 Collection modes (must support)

The DAM solution must support one or more of the following collection approaches, depending on environment and performance needs:

1. **Agentless traffic inspection / proxy monitoring**
   - Capture queries and session context without installing agents on endpoints
   - Enable monitoring of high-volume application traffic while preserving query fidelity
2. **Native audit ingestion (optional / environment-dependent)**
   a. In scenarios where required, support connecting to database native audit sources
   b. Maintain consistent normalization and reporting across sources

Note: Some environments explicitly require avoiding dependence on native audit logs; DAM should be able to operate without them where mandated.

c.2 Central management & scalability

- Central console for configuration, monitoring, and reporting across all monitored databases
- Scale to add new databases without major reconfiguration
- Auto-discover monitored databases and schema objects; detect newly created DB objects

c.3 Performance & resilience

- Operate with minimal overhead and avoid introducing unacceptable latency for database traffic (include measurable overhead targets in acceptance criteria)
- High availability options for high-QPS applications; fail-open or controlled failover patterns for critical workloads

d. Monitoring & Audit Requirements (What must be captured)

d.1 Activity types (must capture)

The DAM solution must capture and classify the full spectrum of database operations, including:

- **Read** activity: SELECT and equivalent query types
- **Write** activity: INSERT/UPDATE/DELETE
- **Schema/administrative** operations: DDL, DCL, grants/revokes, role changes
- Stored procedures / EXEC calls and resulting object access

d.2 Session context captured (must include)

For each event/session, the solution shall record:

- Timestamp
- Database user and/or mapped enterprise identity
- Source host/IP (and application context where applicable)
- Client/tool information (where available)
- SQL command text (or normalized query form) and affected objects (DB/schema/table/column)

d.3 Tamper resistance & audit integrity

- Protect audit logs from DBA manipulation or tampering
- Maintain immutable or controlled-access audit stores and administrative segregation

e. Identity Context & Privilege Controls (DPDP-Critical)

e.1 Identity resolution (must support)

- Resolve service account activity to the individual user behind the application/tool where feasible (e.g., app user context, proxy identity mapping, federated auth traces)

- Enforce separation of duties for DAM administration so no single role can both configure and erase/alter evidence

e.2 Federation & strong authentication (should support)

- Integrate with enterprise identity providers using federation mechanisms (e.g., SAML) and enable SSO/MFA workflows around database access governance where applicable

f. Policy Engine (Data-Aware Controls)

f.1 Policy granularity

Policies shall be configurable at:

- Database instance level
- Schema/table/column level
- User/group/role level
- Application/service account level

f.2 Sensitivity-based logging levels

The solution must allow setting different logging levels by sensitivity of database/object (e.g., higher fidelity logging for personal-data tables).

f.3 Baseline & anomaly policies

Policies should support:

- Thresholds (row counts, query volume, time windows)
- Behavioural baselines per identity/application
- Rare access detection (first-time access to sensitive tables, unusual hours)
- "Break-glass" exceptions with strict audit and expiry

g. Integration with Data Discovery & Classification (Mandatory)

g.1 Column-level sensitivity context

The DAM solution shall ingest classification results to know:

- Which databases contain personal data
- Which tables/columns are classified (e.g., identifiers, financial, citizen/beneficiary data)
- Which datasets are stale but sensitive (higher breach risk)

g.2 Data-aware alert prioritization

Alerts must be prioritized using classification context:

- Access to highly sensitive columns triggers high severity
- Access to stale sensitive data triggers investigation
- Access to unusual sensitive tables triggers rapid containment

h. Threat Detection, Early Warning & Blocking Capabilities

h.1 Detection capabilities (must support)

Detect and alert on:

- Unusual SELECT volumes (mass reads / table dumps)
- Abnormal export patterns (SELECT into files, unusual tooling)
- Suspicious DDL changes (new users/roles, privilege escalation)
- Unexpected schema discovery scans (rapid metadata querying)
- Abnormal deletes/updates affecting sensitive tables

h.2 Prevention & response actions (should support)

Based on policy severity and confidence:

- Terminate suspicious sessions
- Block specific users, roles, or source IPs
- Quarantine or restrict access temporarily (time-boxed)
- Trigger automated workflows in SIEM/SOAR/ticketing tools

i. SOC, SIEM/SOAR & Ticketing Integrations

i.1 Integration requirements

- Forward alerts/events to SIEM, SOAR, and ticketing systems
- Support enrichment fields (data sensitivity, identity confidence, affected objects)
- Support notifications to operational channels (email / collaboration tools)

j. Reporting, Forensics & Evidence (DPDP Audit Readiness)

j.1 Audit reports (must provide)

- User-centric audit: all commands executed by a specific identity
- Object-centric audit: who accessed specific sensitive tables/columns
- DBA and privileged user activity report
- Change tracking report: approved vs unapproved database changes

j.2 Breach triage support

- Rapid identification of affected datasets and identities
- Evidence timelines for investigators
- Exportable, regulator-ready audit packages (immutable logs, event chains)
- DPDP safeguards stress monitoring, detection, and defensible evidence.

k. Integrated Use Cases (Early Detection + Blocking)

Use Case 1 — Compromised user dumps citizen/customer table Signal chain

- Personal Data Access Assurance Solution flags anomalous login

- DAM detects large SELECT bursts on classified personal-data tables
- Classification confirms high sensitivity → severity raised

Response

- Terminate session + disable identity + raise SIEM incident

Outcome

- Stops exfiltration before it becomes a DPDP reportable breach event

Use Case 2 — Service account misuse / app token abuse Signal chain

- DAM detects service account running queries from unusual source IP and executing non-standard query set
- Identity layer resolves context and flags mismatch

Response

- Block source IP / throttle or restrict account, open SOAR workflow

Outcome

- Prevents "trusted" accounts from becoming stealth exfiltration paths

Use Case 3 — DBA attempts to tamper logs after unauthorized query

Signal chain

- DAM records privileged query sequence and detects attempt to disable auditing/alter logs Separation of duties prevents tampering

Response

- Alert high severity; preserve evidence; revoke admin access (via Personal Data Access Assurance Solution)

Outcome

- Maintains DPDP defensibility and preserves chain custody

Use Case 4 — AI assistant triggers iterative enumeration of sensitive columns

Signal chain

- Personal Data intelligent Processing Guard sees repeated prompts / high-rate query requests
- DAM detects schema enumeration + increasing SELECT breadth
- Classification confirms the target columns contain personal data

Response

- Block/slow queries, enforce stricter policies for AI channel, notify SOC

Outcome

AI becomes an early signal for reconnaissance and stops data leakage via "helpful" automation

Use Case 5 — Ransomware precursor: mass delete/alter attempts

Signal chain

- DAM detects abnormal DELETE/UPDATE patterns across many objects
- Personal Data Access Assurance Solution correlates suspicious endpoint/credential behavior

Response

- Terminate sessions, lock accounts, contain blast radius

Outcome

- Early interruption of destructive stage; improved recovery and evidence

5.11 Service Line 11: Digital Personal Data Access Gateway Solution

Attribute	Details
Service Code	SL-11
Deployment Model	SAAS / On-premises / Private Cloud / Hybrid; no personal data to leave department's boundary
Scan Targets	Chrome, Safari, Edge, and Firefox
Classification Framework	Aligned to DPDP Act: Personal Data / Children's Data / Cross-border Flagged
Implementation Timeline	Tool deployed and first scan completed within 5 weeks of Work Order

Scope & Deliverables

a. Purpose & DPDP Compliance Role

a.1 Purpose

The Digital Personal Data Access Gateway Solution shall provide real-time protection at the browser layer to:

- Detect and block malicious and deceptive websites, including pixel-perfect phishing sites
- Prevent credential harvesting, social engineering, and data exfiltration
- Protect users regardless of how links are delivered (email, ads, search, collaboration tools)
- Ensure digital personal data is not disclosed through browser-based attacks

The browser is the final execution point for most modern attacks and the primary channel where personal data is entered, copied, and submitted, making browser-level controls essential for DPDP compliance.

a.2 Why Digital Personal Data Access Gateway Solution Is Mandatory Under DPDP

Under the DPDP Act:

- Unauthorized access or disclosure of digital personal data constitutes a personal data breach

- Data Fiduciaries must implement reasonable, preventive security safeguards
- Reliance on user awareness or static blocklists is insufficient where attackers use deception and impersonation

Modern phishing campaigns now:

- Use near-perfect replicas of trusted sites (including government portals)
- Abuse trusted vendor infrastructure and URL-rewriting services
- Change destinations dynamically to evade traditional controls

Traditional email, network, and signature-based tools cannot reliably detect these threats, making browser-native security a regulatory necessity, not an enhancement.

b. Threat Model Addressed by the Solution

The solution must explicitly protect against:

b.1 Deceptive & Impersonation-Based Attacks

- Pixel-perfect phishing sites impersonating:
  - SaaS login pages
  - Financial institutions
  - Government and law-enforcement portals
- Typosquatted and look-alike domains designed to harvest credentials and personal data

b.2 URL-Rewriting Exploitation

Attackers increasingly:

- Abuse URL-rewriting services of trusted vendors
- Weaponize rewritten links after they are scanned
- Chain multiple redirects through trusted domains to evade detection

Security tools that only check the initial URL or domain reputation fail in these scenarios. The browser must inspect the final destination and rendered page, not just the link.

c. Core Functional Components

1. Browser-Native Inspection Engine
2. AI-Driven Website & Content Analysis
3. Dynamic URL & Redirect Analysis Layer
4. Identity-Linked Risk Context Engine
5. Real-Time Blocking & User Protection Layer
6. Forensics, Audit & Compliance Reporting

d. Browser-Native Threat Detection Capabilities

d.1 Full-Page Visual & Content Inspection

The solution shall:

- Inspect the actual webpage rendered, not just the URL
- Detect malicious intent even when a site:
  - Looks visually identical to a legitimate site
  - Uses correct logos, layouts, and language
- Use computer vision, OCR, and NLP to identify:
  - Credential-harvesting forms
  - Social-engineering language
  - Fake government or security notices

d.2 Zero-Hour Threat Protection

- Inspect every new or previously unseen URL
- Follow all redirects and obfuscation layers
- Emulate real user behavior to expose hidden payloads
- Detect threats that are not yet on any blocklist

e. Multi-Channel Link Protection

The solution must protect users regardless of link origin, including:

- Email
- Search engine results
- Online advertisements
- Social media platforms
- Collaboration tools and chat messages

This ensures **consistent DPDP safeguards** even when attacks bypass traditional email security.

f. Integration with Data Discovery & Classification (Mandatory)

f.1 Data-Aware Risk Evaluation

The Digital Personal Data Access Gateway Solution shall integrate with Data Discovery & Classification to:

- Understand what constitutes personal or sensitive data
- Increase enforcement severity when:
  - Users are about to enter classified personal data into untrusted sites
  - Forms request data types mapped to regulated datasets

This converts phishing protection into personal-data protection, aligning directly with DPDP objectives.

g. Integration with Personal Data Access Assurance Solution:

g.1 Identity-Contextual Protection

The solution shall:

- Associate browser activity with enterprise identities
- Detect abnormal browsing behavior relative to user role
- Elevate risk when:
    - Privileged users encounter credential-harvesting sites
    - Previously compromised identities attempted repeated logins

This enables **early containment** before credential misuse escalates into broader data access.

h. Real-Time Blocking & User Experience

h.1 Enforcement Actions

Upon detecting a malicious or deceptive site, the solution shall:

- Block access **before credentials or data are submitted**
- Present a clear warning explaining the risk
- Provide a safe preview of the blocked content for security teams
- Prevent users from bypassing protection without authorization

i. Integrated Use Cases (Early Detection & Blocking)

Use Case 1 — Fake Government Reporting Site Scenario

- User attempts to report cybercrime
- Lands on a cloned law-enforcement portal
- Page requests extensive personal and organizational data

Outcome

- Digital Personal Data Access Gateway Solution detects visual and contextual impersonation
- Site blocked before data entry

Use Case 2 — URL-Rewriting Phishing Attack Scenario

- User clicks a link rewritten by a trusted security vendor
- Link later redirects to a credential-harvesting page

Outcome

- Digital Personal Data Access Gateway Solution follows the redirect chain
- Inspects the final rendered page
- Blocks the attack despite trusted intermediate domains

Use Case 3 — Compromised Identity Escalation Scenario

- Personal Data Access Assurance Solution flags unusual login behavior
- Same user encounters multiple phishing pages

Outcome

- Digital Personal Data Access Gateway Solution blocks sites
- Personal Data Access Assurance Solution triggers additional verification or session termination

Use Case 4 — Protection Against AI-Generated Phishing Scenario

- AI-generated phishing sites created at scale
- Sites evade static detection due to novelty

Outcome

- Digital Personal Data Access Gateway Solution detects deceptive content via visual and language analysis
- Blocks zero-hour sites

j. Forensics, Reporting & DPDP Evidence

The solution must provide:

- Detailed timelines of user exposure
- Evidence of blocked access and prevented data entry
- High-risk user and campaign summaries
- Regulator-ready reports demonstrating **preventive safeguards**

This supports DPDP accountability and breach-defensibility requirements.

k. Combined Value with Discovery & Personal Data Access Assurance Solution

Capability	Outcome
Data Discovery & Classification	Knows **what** data is sensitive
Personal Data Access Assurance Solution	Knows **who** is accessing
Digital Personal Data Access Gateway	Controls **how and where** data moves

Together, they provide **preventive DPDP compliance**, stopping breaches **before** notification obligations arise.

6. Eligibility & pre-qualification criteria

Bidders must satisfy all pre-qualification criteria. Non-compliance with any mandatory criterion shall result in summary rejection of the bid.

6.1 General Eligibility (All Service Lines)

S#	Criterion	Requirement	Proof
1	Legal Entity	Company / LLP / Partnership / Sole Prop registered in India	CoI / MoA / Partnership Deed
2	GST Registration	Valid GSTIN	GST Certificate
3	PAN	Valid PAN	PAN Card copy
4	Financial Standing	Average Annual Turnover >= Rs. 5 Crore (last 3 FYs); Net Worth positive	Audited P&L, CA Certificate
5	Experience — Privacy/DPDP	Experience of Minimum 1 DPDP complaint or similar services projects in India in the last 5 by bidder or its OEMS.	Copy of Work Orders
6	No Blacklisting	Not blacklisted by any Central/State Govt body	Self-declaration (Annexure B)
7	No Conflict of Interest	Bidder not related to HPSEDC/GOH.P official involved in this RFP	Self-declaration (Annexure B)
8	EMD Submitted	Rs. 1,00,000/- via online payment through E-Procurement portal	Payment receipt

6.2 Service-Specific Eligibility

Under Service specific eligibility criteria, the relevant implementation experience of the bidder or its OEMs in executing similar DPDP-compliant services will be considered.

Service	Minimum Requirement	Key Proof Required
SL-01 (Audit)	DPDP Gap assessment & Audit: Team of minimum 1 qualified privacy professional (CIPP/CIPM/CDPSE/BCI) + 1 legal counsel and Minimum 1 gap assessment projects.	CVs, Certifications, Work Orders
SL-02 (DPO)	Data Protection officer (DPO) as a service: 1 Named DPO with LLB as minimum qualification.	Named DPO CV, Copy of Educational Certifications
SL-03 (CMP)	Consent Management Platform: live deployments in min. 1 organizations (Government/PSU/NBFC/Corporate/Private organization), must demonstrate DPDP-specific consent workflows.	Copy of Work Order/ Purchase order
SL-04 (Discovery)	Data Discovery & Classification Tool: Minimum 1 deployment in Government/PSU/NBFC/Corporate/Private organization regarding Data Discovery & Classification activities.	Copy of Purchase Order
SL-05 (Personal Data access assurance)	Personal Data access assurance Tool: Minimum 1 deployment in Government/PSU/NBFC/Corporate/Private organization regarding Personal Data access assurance activities.	Copy of Purchase Order
SL-06 (Training)	Training and awareness program: Minimum 100 personnel trained on data privacy during the last three (3) years with Learning Management System (LMS) capability supporting bilingual (Hindi & English) training content.	Self-Declaration of Training records and LMS Screenshots
SL-07 (Breach)	Breach response and notification service: Demonstrated 24×7 Security Operations Centre (SOC) capability with a named Digital Forensics and Incident Response (DFIR) Lead with GCFE/GCFA/CISM certification having relevant experience in incident response and digital	SOC documentation, DFIR CV and copy of GCFE/GCFA/CISM certification

	forensics.	
L-08 (Data loss prevention)	Data Loss Prevention Solution: Minimum 1 deployment of Government/PSU/NBFC/Private/Corporate Enterprises; Or relevant implementation experience of the bidder or its OEMS in executing same or similar DPDP-compliant services	Copy of Purchase order
SL-09	Personal Data Intelligent Processing Guard Solution	Product screenshot/Brochure
SL-10	Database Activity Monitoring Solution: Minimum 1 deployment in Government/PSU/NBFC/Corporate/Private organization.	Copy of Purchase order
SL-11	Digital Personal Data Access Gateway Solution: Minimum 1 deployment in Government/PSU/ NBFC/Corporate/Private organization regarding Digital Personal Data Access Gateway Solution	Copy of Purchase order

7. Bid process & schedule

7.1 Bid Structure

Bidders must submit a Two-Part Bid on the e-procurement portal:

a) Technical Bid: Complete technical response, eligibility documents, CVs, references, and all Annexures except Annexure D.

b) Financial Bid (Rate Card): Completed Annexure D with rates for all service lines bid for. Financial Bid shall not be opened until Technical Bid evaluation is complete.

7.2 Bid Submission Requirements

7.2.1 All documents must be submitted online at hptenders.gov.in Physical bids shall not be accepted.

7.2.2 Documents must be uploaded in PDF format. Size limit per document: 15 MB.

7.2.3 Bids must be digitally signed using DSC (Digital Signature Certificate) of Class 3 — Organization category.

7.2.4 The Bid Submission Checklist (Annexure A) must be completed and uploaded as the first document.

7.2.5 Financial Bid (Annexure D) must be uploaded separately in the designated Financial Bid.

7.2.6 Late bids shall not be accepted by the portal system.

8. Evaluation methodology

8.1 Evaluation Framework

Minimum qualifying technical score: 60 out of 100. Bidders scoring below 60 shall not have their financial bid opened.

8.2 Technical Evaluation Criteria

Under Technical Evaluation criteria the relevant implementation experience of the bidder or its OEMS in executing similar DPDP-compliant services will be considered.

S#	Criterion	Max Marks	Scoring Guidance
	A. ORGANISATIONAL CAPABILITY	**30**	
A1	Years in business	15	• Up to 3 years: 5 Marks • More than 3 years up to 5 years: 8 Marks • More than 5 years up to 10 years: 10 Marks • More than 10 years: 15 Marks

A2	Team size of IT professionals (Self-Declaration of bidders on letterhead)	5	• Up to 25 Team size: 1 Mark • More than 25 Team size up to 50 Team size: 3 Marks • More than 50 Team size: 5 Marks
A3	ISO 27001, CERT-IN empanelment (Relevant certification of bidder or its OEMS will be considered)	5	• None: 0 Mark • ISO 27001 only: 3 Marks • CERT-IN: 5 Marks
A4	Financial turnover (last 3 FYs average)	5	• Rs.5-10Cr: 3 Marks • More than Rs.10Cr: 5 Marks
	B. RELEVANT EXPERIENCE	**35**	
B1	DPDP/Privacy Gap Assessments Projects Or relevant implementation experience of the bidder or its OEM's in executing same.	5	• 1 Project: 2 Marks • 2 Projects: 3 Marks • 3 Projects: 5 Marks
B2	DPO / Advisory Assignments (ongoing or completed) Or relevant implementation experience of the bidder or its OEM's in executing same.	5	• 1 Project: 2 Marks • 2 Projects: 3 Marks • 3 Projects: 5 Marks
B3	CMP deployments in production or relevant implementation experience of the bidder or its OEM's in executing same.	5	• 1 Project: 2 Marks • 2 Projects: 3 Marks • 3 Projects: 5 Marks
B4	Data Discovery tool deployments in Government / PSU / Corporate / Private organization. Or relevant implementation experience of the bidder or its OEM's in executing same.	4	• 1 Project: 2 Marks • 2 Projects: 4 Marks
B5	Personal Data Access Assurance Solution in Government / PSU / Corporate / Private organization. Or relevant implementation experience of the bidder or its OEM's in executing same.	4	• 1 Project: 2 Marks • 2 Projects: 4 Marks
B6	Data Loss Prevention Solution Or relevant implementation experience of the bidder or its OEMS in executing same.	4	• 1 Project: 2 Marks • 2 Projects: 4 Marks
B7	Database Activity Monitoring Solution in Government / PSU / Corporate / Private organization Or relevant implementation experience of the bidder or its OEMS in executing same.	4	• 1 Project: 2 Marks • 2 Projects: 4 Marks
B8	Digital Personal Data Access Gateway Solution in Government / PSU / Corporate / Private organization Or relevant implementation experience of the bidder or its OEMS in executing same.	4	• 1 Project: 2 Marks • 2 Projects: 4 Marks
	C. TECHNICAL SOLUTION QUALITY	**25**	
C1	Quality of Technical Proposal & Methodology	10	Evaluated by Committee
C2	Tool/Platform Demo Quality (SL-03, SL-04, SL-05, SL-06,SL-08, SL-09, SL-10, SL-11)	10	Live demo scored by Committee against checklist
C3	Data residency & security architecture	5	• India-resident on NIC/MeitY cloud: 5 Marks • Other: 2-4 Marks
	D. Himachal Pradesh (H.P) PRESENCE	**10**	
D1	Office / delivery center in H.P (Copy of GST/Rent agreement)	5	• Office in H.P: 5 Marks • None: 0
D2	Prior GOH.P / HPSEDC engagement (Any IT-related project involving software development, IT technical manpower, or cybersecurity services.)	5	• 2 projects: 5 Marks • 1 project: 3 Marks • None: 0

8.3 Financial Evaluation & Selection Criteria

8.3.1 Only those bidders who are found **technically qualified** as per the Technical Evaluation Criteria shall be considered for financial evaluation and empanelment.

8.3.2 All technically qualified bidders shall be eligible for empanelment, subject to meeting all tender

conditions and submission of the required documents.

8.3.3 The **lowest quoted rate (L1)** received for each individual **Service Line** among the technically qualified bidders shall be considered as the **Final Rate Contract** for that respective Service Line.

8.3.4 All technically qualified bidders seeking empanelment shall be required to submit their **written consent** to provide the respective Service Line(s) at the **L1 rate** finalized by HPSEDC. The consent shall be submitted in the prescribed format within the stipulated time.

8.3.5 Only those technically qualified bidders who provide their unconditional consent to match and accept the **L1 rate** for the respective Service Line(s) shall be empaneled and shall be eligible for award of work/orders during the validity of the empanelment.

8.3.6 In the event that a technically qualified bidder declines or fails to submit the required consent within the stipulated period, the bidder shall not be considered for empanelment.

8.4 Empanelment Decision

a) All bidders who will provide their unconditional consent to match and accept the L1 rate for all service line shall be empaneled on the Rate Contract.

b) There is no single-winner outcome. Multiple agencies shall be empaneled, enabling departments to choose.

c) Empaneled agencies shall be publicly listed on the HPSEDC DPDP Rate Contract portal with the rates, service lines, and performance ratings.

9. Financial bid structure & rate card

Bidders must complete Annexure D (Rate Card Template) for all service lines. The Rate Card shall define the ceiling rates that shall be published on the HPSEDC portal. Actual Work Orders may be at or below these rates.

NOTE: All rates must be quoted inclusive of all professional fees, travel (within H.P), tools, licenses, and expenses. GST shall be charged separately @18% rates. Quoted rates shall remain firm for 3 years from Rate Contract signing.

(Any change in applicable GST rate shall be applicable to the bidder.)

9.1 Travel & Out-of-Pocket Expenses

a) Travel within H.P: Must be included in quoted rates — no separate billing allowed.

b) Travel outside H.P / International: If required by a specific Work Order, actual costs (economy class, per department approval) to be reimbursed as pass-through. Prior written approval required.

c) Accommodation: As per GOH.P TA/DA rules applicable to the equivalent grade official. Receipts are mandatory.

10. Service level agreements (Slas)

10.1 Response & Delivery SLAs

Code	Service	KPI	Target	Penalty for Breach
SL-01	Gap Assessment	Report delivery from Work Order	8 weeks	1% of order value/week delay
SL-02	DPO Service	Response to department query	4 business hours	Rs.5,000/instance > 5 breaches/month
SL-02	DPO Service	DSAR response managed	30 days (per Act)	Rs.10,000 per delayed DSAR
SL-03	CMP Platform	Platform uptime	99.5%/month	10% monthly fee per 0.5% shortfall
SL-03	CMP Platform	Go-live from Work Order	12 weeks	1.5% order value/week delay
SL-04	Discovery Tool	First scan completion	5 weeks from WO	1% order value/week delay
SL-04	Discovery Tool	Dashboard refresh	Weekly	Rs.2,000/missed cycle

SL-05	Training	Program commencement from WO	4 weeks	Rs.5,000/week delay
SL-05	Training	Completion rate achieved	>= 90%	Redelivery at no cost
SL-06	Breach Response	Incident acknowledgement	Within 1 hour (24x7)	Rs.10,000/hour breach
SL-06	Breach Response	Preliminary assessment	Within 4 hours of acknowledgement	Rs.10,000/hour
SL-06	Breach Response	DPBI initial notification filed	Within 72 hours of breach discovery	Rs. 50,000 flat breach
SL-06	Breach Response	Post-Incident Review report	30 days post-incident	Rs.5,000/day delay
SL-07	Personal Data Access Assurance Solution	Integration of Access Assurance tool with Data Discovery tool & Identity Mapping	07 days from project Kick off	Rs.5,000/day delay
SL-08	Data Loss Prevention Solution	Integration of Access Assurance tool with Data Discovery tool	14 days from project Kick off	Rs.5,000/day delay
SL-09	Personal Data intelligent Processing Guard	Integration of Access Assurance tool with Data Discovery tool	14 days from project Kick off	Rs.5,000/day delay
SL-10	Database Activity Monitoring Solution	Integration of Access Assurance tool with Data Discovery tool & Database Integration	60 days from project Kick off	Rs.5,000/day delay
SL-11	Digital Personal Data Access Gateway Solution	Integration of Access Assurance tool with Data Discovery tool and Endpoint Deployment	07 days from project Kick off	Rs.5,000/day delay

10.2 Reporting Obligations

a) Monthly Service Report: All active service lines reports to department DPO / Nodal Officer by 5th of each month.

b) Quarterly Portfolio Report to HPSEDC: Across all active Work Orders — SLA performance, open issues, escalations.

11. General terms & conditions

11.1 Intellectual Property Rights

a) All reports, assessments, policies, training materials, code, configurations, and deliverables produced specifically for GOH.P entities under Work Orders shall vest in the respective Government entity.

b) Agencies must not use GOH.P data or insights for marketing, benchmarking, research publications, or any third-party purpose without prior written consent of HPSEDC/GOH.P.

11.2 Confidentiality & Data Security

a) Agencies shall treat all information received from GOH.P entities as strictly confidential. Signed NDAs (Annexure E) are mandatory before commencement of any work.

b) Agencies shall implement controls consistent with Rule 6 of the DPDP Rules 2025 for any personal data accessed during service delivery.

c) Data shall not be transferred outside India without HPSEDC written approval.

d) Upon expiry or termination of a Work Order, agencies shall irreversibly delete or return all GOH.P data within 30 days and provide a deletion certificate.

11.3 Audit & Inspection Rights

a) HPSEDC and GOH.P entities reserve the right to audit the agency's delivery service processes, records, and systems at any time with 7 days' notice.

b) Agencies shall maintain records of all Work Orders, deliverables, and communications for a

minimum of 7 years from the Rate Contract end date.

11.4 Subcontracting

a) Sub-contracting is not permitted without prior written approval from the concerned department and HPSEDC.

b) Approved sub-contractors must satisfy equivalent eligibility criteria. The prime agency remains fully liable.

c) Sub-contracting to entities blacklisted by any Government is strictly prohibited.

11.5 Key Personnel

a) Key personnel proposed in the Technical Bid may not be replaced without prior 15-day notice and HPSEDC approval.

b) Replacement personnel must have equal or higher qualifications than those proposed.

c) The bidder shall ensure uninterrupted continuity of work throughout the transition and handover process, with no disruption to ongoing services.

12. Payment terms

12.1 Payment Schedule by Service Line

Code	Service	Payment Milestones
SL-01	Gap Assessment & Audit	30% on Project Kick off | 50% on draft report accepted | 20% on final report accepted
SL-02	DPO-as-a-Service	Monthly in arrears on submission of activity report and department sign-off
SL-03	Consent Management Platform	40% on go-live | 20% at 3 months | 20% at 6 months | 20% at 12 months
SL-04	Data Discovery Tool	30% on deployment | 30% on first scan report | 40% on department acceptance
SL-05	Training	60% on completion of each module batch | 40% on final effectiveness report
SL-06 (Retainer)	Breach Response Retainer	Quarterly in advance
SL-07	**Personal Data Access Assurance Solution**	30% on deployment | 30% on first scan report | 40% on department acceptance
SL-08	**Data Loss Prevention Solution**	30% on deployment | 30% on first scan report | 40% on department acceptance
SL-09	Personal Data intelligent Processing Guard	30% on deployment | 30% on first scan report | 40% on department acceptance
SL-10	Database Activity Monitoring Solution	30% on deployment | 30% on first scan report | 40% on department acceptance
SL-11	Digital Personal Data Access Gateway Solution	30% on deployment | 30% on first scan report | 40% on department acceptance

12.2 Payment Processing

a) Payments shall be made by the respective GOH.P Department/Entity (not HPSEDC) directly to the agency within 30 days of invoice submission and acceptance of deliverables.

b) TDS shall be deducted as applicable under the Income Tax Act 1961. GST Input Tax Credit shall be passed to the concerned department.

c) Invoices must be submitted on the department's ERP/finance portal (where applicable) or physically addressed to the designated Pay & Accounts Officer.

d) Disputed invoices shall be resolved within 15 days by the department's Nodal Officer. Undisputed amounts must be paid within 30 days.

13. Penalties & liquidated damages

13.1 Liquidated Damages

Liquidated damages shall apply for delays in delivery/performance as specified in Section 10.1. Total LD shall not exceed 05% of the Work Order value. LD shall be deducted from the next invoice.

13.2 Penalties for non-compliance

Event	Penalty	Recovery Method
Unauthorized use or breach of GOH.P/citizen data by agency	Up to Rs. 10,00,000	Performance Security
Failure to notify HPSEDC of agency's own data breach within 48 hours	Rs. 1,00,000 flat	Invoice deduction
Misrepresentation in bid documents	Disqualification + forfeiture of EMD	EMD
Failure to maintain agreed SLAs for 3 consecutive months	Show Cause Notice	HPSEDC action
Failure to submit quarterly report to HPSEDC	Rs. 5,000 per delayed report	Invoice deduction

13.3Suspension & Removal from Rate Contract

HPSEDC may suspend an agency from the Rate Contract for:

a) Criminal charges or legal proceedings related to data privacy/fraud.

b) Blacklisting by any Central/State Government entity during the contract period.

c) Material misrepresentation in the bid or during contract execution.

Suspension shall be for a minimum of 6 months. Re-instatement requires HPSEDC committee review and remediation evidence.

14. Governing law & dispute resolution

14.1 Governing Law

This Rate Contract and all Work Orders issued thereunder shall be governed by and construed in accordance with the laws of India, including the Digital Personal Data Protection Act 2023, the Information Technology Act 2000, the Indian Contract Act 1872, the General Financial Rules 2017, and the H.P Financial Rules 2009.

14.2 Dispute Resolution

a) Amicable Resolution: Parties shall first attempt resolution by mutual discussion within 30 days of written notice of dispute.

b) Resolution by Authorised Representatives: If not resolved, the parties shall attempt resolution through their respective authorised representatives within 45 days.

c) Arbitration: In case the dispute remains unresolved, either party may invoke arbitration in accordance with the Arbitration and Conciliation Act, 1996, as amended from time to time. The dispute shall be referred to a **sole arbitrator mutually appointed by the parties**. Failing mutual agreement within 30 days, the arbitrator shall be appointed in accordance with **Section 11 of the Act**. The **seat of arbitration shall be Shimla, Himachal Pradesh**, and proceedings shall be conducted in English.

d) Courts: Courts of competent jurisdiction in Shimla, Himachal Pradesh shall have exclusive jurisdiction for matters not covered by arbitration.

14.3 Force Majeure

Force majeure events (natural disasters, war, pandemics, government orders) excusing performance must be notified in writing within 72 hours. The party invoking force majeure must demonstrate direct impact. Work Order timelines shall be extended for the force majeure period. No financial compensation shall be due for force majeure periods.

ANNEXURE A: BID SUBMISSION CHECKLIST

Bidders must complete this checklist and upload it as the first document in their Technical Bid . Incomplete submissions may be rejected.

S#	Document	Included (Y/N)	Page Ref
1	Annexure A — This completed Checklist		
2	Annexure B — Bidder Profile & Declaration (signed & stamped)		
3	Certificate of Incorporation / LLP Agreement / Partnership Deed		
4	Valid GSTIN Certificate		
5	PAN Card of Organization		
6	Audited Financial Statements (last 3 FYs)		
7	CA Certificate for Average Turnover		
8	EMD Payment Receipt		
9	Annexure C — Technical Capability Statement		
10	Relevant Work Orders + Client Completion Certificates (min. 2)		
11	CVs of Key Personnel (DPO, Lead Auditor, DFIR Lead)		
12	Copies of Professional Certifications (CIPP/CIPM/CDPSE/GCFE/etc.)		
13	ISO 27001 / CERT-IN empanelment certificate (if applicable)		
14	Tool / Platform product brochure or demo video link (SL-03, SL-04)		
15	UDYAM Registration Certificate (for MSMEs)		
16	Signed NDA (Annexure E) — to be submitted at empanelment stage		
17	Annexure D — Financial Bid (Rate Card) — uploaded in Financial Bid ,ONLINE ONLY		

ANNEXURE B: BIDDER PROFILE & DECLARATION

Part I — Bidder Profile

Field	Response
Legal Name of Bidder / Lead Entity	
Type of Entity (Pvt Ltd / LLP / Partnership)	
CIN / LLP Registration No.	
Date of Incorporation	
Registered Address	
Principal Place of Business / Operations HQ	
GSTIN	
PAN	
UDYAM No. (if MSME)	
Average Annual Turnover (last 3 FYs, Rs. Crore)	
Authorised Signatory Name & Designation	
Email Address for Correspondence	
Mobile / Phone	

Part II — Declarations

We, the undersigned, hereby solemnly declare that:

k) All information provided in this bid is true, accurate, and complete. We understand that any misrepresentation shall result in disqualification and potential legal action.

l) Our organization is not blacklisted by any Central Government, State Government, PSU, or International Development Institution.

m) None of our directors, partners, or key personnel are government servants of GOH.P or are relatives of any HPSEDC official involved in this procurement.

n) We accept all terms and conditions of this RFP without qualification or exception, unless expressly noted in our bid.

o) We understand that the Rate Contract does not guarantee any minimum volume of work.

p) We agree to maintain the validity of our bid for 180 days from the date of opening of commercial offers.

q) We confirm that we have the requisite authorizations, licenses, and legal standing to provide the proposed services.

Authorized Signatory:

Name: _____

Designation: _____

Date: _____

Company Seal & Signature:

(Affix company seal and sign)

ANNEXURE C: TECHNICAL CAPABILITY STATEMENT

Bidders shall complete this statement for each Service Line bid for. Attach supporting evidence for each entry.

C— Key Personnel Proposed

Role	Name	Qualifications	Certifications	Years Relevant Exp.
Lead DPO				
Lead Auditor (SL-01)				
CMP Technical Lead (SL-03)				
DFIR Lead (SL-06)				
Training Lead (SL-05)				
Project Manager				

C.1 — Relevant Projects / References

S#	Client Name	Service Line(s)	Contract Value	Period	Contact for Reference
1					
2					
3					
4					
5					

C.2 — Infrastructure & Tools Declared

i) Data Centre / Cloud: _____

j) CMP Platform Name & Version: _____

k) Data Discovery Tool Name: _____

l) SIEM / SOC Platform (for SL-06): _____

m) LMS Platform (for SL-05): _____

n) ISO 27001 Certificate No. & Validity: _____

o) CERT-IN Empanelment No. (if applicable): _____

ANNEXURE D: FINANCIAL BID / RATE CARD TEMPLATE

NOTE: This Annexure must be uploaded ONLINE ONLY in the Financial Bid. Do not include price information anywhere in the Technical Bid. Rates quoted must be in Indian Rupees (INR), exclusive of GST.

(To be submitted by the bidder- ONLINE ONLY)

To

Managing Director

H.P State Electronics Development Corporation Limited (HPSEDC)

1st FLOOR, I.T BHAWAN, MEHLI, SHIMLA-171013, H.P.

Subject: HPSEDC/HP/2026-27/3372

I/We hereby tender for the _____ and provision of services during the warranty period, as per the specifications given in this Tender document within the time specified and in accordance with the specifications and instructions. Mentioned below are the rates quoted in the prescribed format are FOR destination inclusive of all taxes: -

Code	Service Line	Unit	Basic Rate (Rs.)	GST %
SL-01A	Gap Assessment — Small Dept (up to 1000 staff)	Per engagement		18%
SL-01B	Gap Assessment — Medium Dept (1001-5000 staff)	Per engagement		18%
SL-01C	Gap Assessment — Large Dept (more than 5000 staff)	Per engagement		18%
SL-01D	Annual Re-Audit (SDF)	Per dept / per year		18%
SL-02A	DPO-as-a-Service (Shared)	Per dept / per month		18%
SL-02B	DPO-as-a-Service (Dedicated)	Per dept / per month		18%
SL-03A	CMP SaaS — Small (up to 1L users)	Per dept / per year		18%
SL-03B	CMP SaaS — Medium (1L-5L users)	Per dept / per year		18%
SL-03C	CMP SaaS — Large (more than 5L users)	Per dept / per year		18%
SL-03D	CMP Implementation (one-time)	Per engagement		18%
SL-04A	Data Discovery — Small (up to 10 TB)	Per engagement (one-time)		18%
SL-04B	Data Discovery — Medium (10-100 TB)	Per engagement (one-time)		18%
SL-04C	Data Discovery — Large (more than 100 TB)	Per engagement (one-time)		18%
SL-04D	Data Discovery — Annual License / Scan	Per dept / per year		18%
SL-05A	Training — e-Learning per learner per module	Per learner per module		18%
SL-05B	Training — In-person workshop	Per training day (≤30 pax)		18%
SL-05C	Training — In-person workshop	Per training day for each additional 5 participants beyond 30.		18%

Code	Service Line	Unit	Basic Rate (Rs.)	GST %
SL-05D	LMS Hosting (annual)	Per dept / per year		18%
SL-06A	Breach Response — Annual Retainer	Per dept / per year		18%
SL-07 (A)	**Personal Data Access Assurance:** Per department engagement (up to 5000 users)	Per engagement		18%
SL-07 (B)	**Personal Data Access Assurance:** Per department engagement (5001-10000 users)	Per engagement		18%
SL-07 (C)	**Personal Data Access Assurance:** Per department engagement (more than 10000 users)	Per engagement		18%
SL-08(A)	**Data Loss Prevention Solution** Per department engagement (up to 5000 User)	Per engagement		18%
SL-08(B)	**Data Loss Prevention Solution** Per department engagement (5001-10000 User)	Per engagement		18%
SL-08(C)	**Data Loss Prevention Solution** Per department engagement (more than 10000 User)	Per engagement		18%
SL-09(A)	**Personal Data intelligent Processing Guard** (Per department engagement (1 AI Platform)	Per engagement		18%
SL-09(B)	**Personal Data intelligent Processing Guard** (Per Department engagement 2-5 AI Platform)	Per engagement		18%
SL-9(C)	**Personal Data intelligent Processing Guard** (Per department engagement (6-10 AI Platform)	Per engagement		18%
SL-10(A)	**Database Activity Monitoring Solution Per department engagement** (up to 5 Databases)	Per engagement		18%
SL-10(B)	**Database Activity Monitoring Solution Per department engagement** (6-50 Databases)	Per engagement		18%
SL-10(C)	**Database Activity Monitoring Solution Per department engagement** (51- 100 Databases)	Per engagement		18%
SL-11(A)	**Digital Personal Data Access Gateway Solution** (Per department engagement (more than 5000 user)	Per engagement		18%
SL-11(B)	**Digital Personal Data Access Gateway Solution** (Per department engagement (5001-10000 user)	Per engagement		18%
SL-11(C)	**Digital Personal Data Access Gateway Solution** (Per department engagement (more than 10000 user)	Per engagement		18%

The bid found in any other currency shall be summarily rejected.

No upward revision shall be allowed in the case of any fluctuation in the foreign currency

1. Period of Delivery: We do hereby undertake that in the event of acceptance of our bid, the supply of mentioned items will be completed within stipulated delivery period as motioned in RFP from the date of issues of purchase order unless otherwise specified in the purchase order.

2. Terms of Delivery: The landed prices quoted are inclusive of applicable taxes and duties.

3. We agree to abide by our offer for a period of 180 days from the date of opening of commercial offers and that we shall remain bound by a communication of acceptance within that time.

4. We hereby certify that we have read and understood the terms and conditions applicable to the bidder and we do hereby undertake to supply as per these terms and conditions.

5. A company and the person signing the bid/offer is the constituted attorney.

NOTE: Delete whatever is not applicable. All corrections/deletions should invariably be duly attested by the person authorized to sign the bid/offer document.

We certify that the rates quoted above are our best and final rates for the HPSEDC Rate Contract, inclusive of all costs except GST, and shall remain valid for the contract period as stated in this RFP.

Yours Sincerely,

Authorized Signatory (ies)[In full and initials]: _____

Name and Title of Signatory (ies): _____
Name of Bidding Company/Firm: _____
Address: _____*(Affix the Official Seal of the Bidding Company)*

ANNEXURE E: NON-DISCLOSURE AGREEMENT (TEMPLATE)

This Non-Disclosure Agreement ('NDA') is entered into on [DATE] between:

1. HPSEDC

H.P State Electronics Development Corporation Limited,

HPSEDC 1st Floor, I.T. Bhawan,

Mehli, Shimla-171013,

acting on behalf of [NAME OF DEPARTMENT] ('Disclosing Party')

AND

1. [AGENCY NAME]

[Registered Address] ('Receiving Party')

Key NDA Terms

- **a)** Confidential Information: All personal data, citizen records, IT architecture, security configurations, policy drafts, legal advice, and business processes of GOH.P/HPSEDC/Department.
- **b)** Obligation: Receiving Party shall not disclose Confidential Information to any third party; shall use it solely for service delivery under the Rate Contract Work Order; shall implement security controls per DPDP Rules 2025 Rule 6.
- **c)** Duration: 5 years from NDA signing + indefinite for personal data of citizens.
- **d)** Data Return: All Confidential Information (physical and digital) shall be returned or irreversibly destroyed within 30 days of Work Order expiry. Deletion Certificate to be provided.
- **e)** Governing Law: Laws of India; jurisdiction: Courts of Himachal Pradesh.

[FULL NDA TEXT MAY BE FINALISED BY HPSEDC LEGAL TEAM AT THE TIME EMPLANEMENT]

Annexure F: Self-Declaration on not being blacklisted

(To be enclosed with technical bid)

Date: _____

Subject: HPSEDC/HP/2026-27/3372

From

_____

_____

To
The Managing Director,
H.P State Electronics Development Corporation 1st
FLOOR, I.T BHAWAN, MEHLI, SHIMLA-171013, H.P.

I, _____son of Sh. _____ resident of _____do hereby solemnly affirm and declare as under: -

That we M/s _____ hereby confirm that we M/s_____ has not been blacklisted by any State Government/ Central Government/ Public Sector Undertakings.

That we M/s_____ hereby declare that all the particulars furnished by us in this Tender are true to the best of my/our knowledge and I/We understand and accept that if at any stage, the information furnished is found to be incorrect or false, I/We am/ are liable for disqualification from this tender and also are liable for any penal action that may arise due to the above.

That we M/s _____certify that no refurbished components are used in the manufacturing and supply of Quoted Items and its related accessories / tendered items.

That in case of violation of any of the conditions above, We M/s _____ understand that We M/s _____are liable to be blacklisted by HPSEDC for participating any tender published by H.P Government.

DEPONENT

Verification:
Verified that the contents of the above affidavit of mine are true and correct to the best of my knowledge and nothing has been concealed therein.

DEPONENT

Annexure H: Certificate of Authorization Certificate

(To be provided by the OEM of the software, products or solutions on OEM's letterhead) to be enclosed with technical bid

Dated: _____

Managing Director
H.P State Electronics Development Corporation Limited (HPSEDC)
1st FLOOR, I.T BHAWAN, MEHLI, SHIMLA-171013, H.P.

Subject: HPSEDC/HP/2026-27/3372

Sir,

This is to certify that I/We are the OEM/authorized entity for the software, products or solutions listed below and confirm that <Name of Bidder> is duly authorized to provide the same and the associated licensing, support, maintenance and upgrades.

- <Name of Bidder> have due authorization from us to provide software, products or solution(s) listed below.
- We endorse the updates/upgrades/support, contracting and licensing terms provided by <Bidder> as per the requirement of this tender.
- We further undertake that we as an OEMS of the below-mentioned software solution will discharge all responsibilities under applicable support for the period indicated in the contract/purchase order, in case the Bidder fails to do the same for any reason.
- We also certify that the below-mentioned product/software solution(s) being supplied by the <Bidder> meets the minimum specifications given in the Tender document.

The authorization will remain valid till <*Date of renewal of dealership*>

S#	Product/Software Solution Name
1	<*Fill* Product/Software Solution *name*>
2	…

Authorized Signatory (ies) [In full and initials]: _____
Name and Title of Signatory (ies): _____
Name of Bidding Company/Firm: _____
Address: _____*(Affix the Official Seal of the Bidding Company)*

Annexure I: Undertaking for honoring warranty/support for the period indicated in the contract

(To be enclosed with technical bid and to be submitted by the bidder on OEMS letter head)
Dated: -

Managing Director
H.P State Electronics Development Corporation Limited (HPSEDC)
1st FLOOR, I.T BHAWAN, MEHLI, SHIMLA-171013, H.P.

Subject: HPSEDC/HP/2026-27/3372

This bears reference to our quotation Ref. _____Dated _____

We undertake that,

1) All software, solutions, products or services supplied/provided by <Name of Bidder> shall conform to the specifications and applicable requirements of the Tender and shall be supported for the period specified in the Contract/Work Order.
2) We shall provide the applicable license/subscription, OEM authorization and support/maintenance documentation, wherever applicable, at the time of deployment.
3) We shall provide applicable support, updates, patches and upgrades required for continued functionality and security during the contracted support period.
4) We shall provide reasonable advance notice of any **end-of-support/end-of-life** and provide an appropriate upgrade, supported version or migration path, wherever applicable, without adversely affecting service continuity.
5) In case the proposed solution becomes unsupported during the contract period, we shall provide an equivalent or upgraded supported solution, wherever applicable, without additional cost and without adversely affecting the agreed functionality or timelines.

Authorized Signatory (ies)[In full and initials]: _____
Name and Title of Signatory (ies): _____
Name of Bidding Company/Firm: _____
Address: _____*(Affix the Official Seal of the Bidding Company)*

Annexure J: Authenticity of submitted documents/information's

(Self-declaration to be submitted by bidder on their company letter)

Subject: HPSEDC/HP/2026-27/3372

Affidavit of Mr..... S/o ..... R/o .....
I, the deponent above named do hereby solemnly affirm and declare as under:

1. That I am the Proprietor/Authorized signatory of M/s ……. Having its Head Office/Regd. Office at ……..
2. That the information/documents/Experience certificates submitted by M/s……. along with the tender for …… *(Name of work*) to the Corporation are genuine and true and nothing has been concealed.
3. I shall have no objection in case the Corporation verifies them from issuing authority (ies). I shall also have no objection in providing the original copy of the document(s), in case the Corporation demand so for verification.
4. I hereby confirm that in case, any document, information & / or certificate submitted by me found to be incorrect / false / fabricated, the Corporation at its discretion may disqualify / reject / terminate the bid/contract and also forfeit the EMD / All dues.

I, ..., the Proprietor / Authorised signatory of M/s .....do hereby confirm that the contents of the above.
Affidavit are true to my knowledge and nothing has been concealed there from. ..... and that no part of it is false.

Verified at .....this.....day of .....

DEPONENT

ATTESTED BY (NOTARY PUBLIC)

Appendix 1: Request for clarification

Bidders requiring specific points of clarification may communicate with the HPSEDC through email during the specified period using the following format.

Date: _____

To
Managing Director
H.P State Electronics Development Corporation Limited (HPSEDC)
1st FLOOR, I.T BHAWAN, MEHLI, SHIMLA-171013, H.P.

Subject: HPSEDC/HP/2026-27/3372

BIDDER'S REQUEST FOR CLARIFICATION			
<<*Name of Bidder submitting query / request for clarification*>>			
<<*Full formal address of the Bidder*>>			*Tel:*
			Fax:
			Email:
S. No	RFP Reference (Section No. / Page No.)	Content of RFP requiring clarification	Points of clarification required
1			
2			
3			
4			
5			
6			

Authorized Signatory [In full initials]: _____

Name and Title of Signatory: _____
Name of Bidding Company/Firm: _____
Address: _____*(Affix the Official Seal of the Company)*