FDPPI STANDARD ENGAGEMENT AGREEMENT

Engagement of Independent Data Auditor (IDA)

Recommended Model Contract — Version 2.0 (2026 Edition)

This Agreement is made on: ___ day of _____ 20___	**Agreement Reference No.:** _____
Data Fiduciary (Full Legal Name): _____ CIN / Registration No.: _____	**Independent Data Auditor (Full Legal Name):** _____ AIDAI Empanelment No.: _____

WHEREAS, the Data Fiduciary is engaged in processing of personal data as a Data Fiduciary within the meaning of the Digital Personal Data Protection Act, 2023 ("DPDPA") and desires to engage an empanelled Independent Data Auditor to assess, review and report upon its data protection and compliance posture;

AND WHEREAS, the Auditor is duly empanelled with the Association of Independent Data Auditors of India ("AIDAI") under the Foundation of Data Protection Professionals in India ("FDPPI") and possesses the requisite professional competence, independence and ethical standing to conduct such audit;

NOW THEREFORE, in consideration of the mutual covenants herein and for good and valuable consideration, the sufficiency of which is hereby acknowledged, the Parties agree as follows:

1. Definitions and Interpretation

In this Agreement, the following terms shall have the meanings ascribed to them below:

AIDAI	Association of Independent Data Auditors of India, a Voluntary professional body governing empanelment and ethical conduct of Independent Data Auditors.
Audit Period	The period commencing from the date of this Agreement until delivery of the Final Audit Report or as specified in Annexure B.
Confidential Information	All non-public information, data, trade secrets, business processes, technical documentation, and personal data encountered during the audit engagement.
Data Fiduciary	A person or entity that determines the purpose and means of processing of personal data, as defined under Section 2(i) of the DPDPA 2023.
DPDPA 2023	The Digital Personal Data Protection Act, 2023, including all rules and regulations made thereunder, as amended from time to time.
DPB	Data Protection Board of India, established under Section 18 of the DPDPA 2023.

FDPPI	Foundation of Data Protection Professionals in India, the apex body that has developed and maintains the DGPSI framework and governs AIDAI.
IDA / Auditor	The Independent Data Auditor engaged under this Agreement, being a person or firm duly empanelled with AIDAI.
Personal Data Breach	Any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.
Significant Data Fiduciary	A Data Fiduciary recognized as such under Section 10 of the DPDPA 2023.

1.2 Unless the context otherwise requires: (a) references to any statute include all subordinate legislation made thereunder; (b) words in the singular include the plural and vice versa; (c) headings are for convenience only and shall not affect interpretation.

2. Objective and Scope of Audit

2.1 Objective

The primary objective of this engagement is to conduct an independent, risk-based audit of the Data Fiduciary's data governance architecture, data protection practices, and regulatory compliance posture, culminating in a professional opinion and actionable recommendations.

2.2 Scope of Work

The scope of the audit shall include, but not be limited to:

- Compliance assessment against DPDPA 2023, including obligations on consent, notice, data principal rights, and grievance redressal;
- Review of data processing activities, records of processing, data flow mapping, and lawful bases;
- Evaluation of technical and organisational security safeguards, including encryption, access controls, and breach response capabilities;
- Assessment of data retention and deletion policies and their operational implementation;
- Review of contracts with Data Processors and sub-processors for compliance with Section 8(2) of DPDPA 2023 ;
- Examination of internal policies, standard operating procedures, audit logs, and privacy governance documentation;
- Assessment of data principal rights fulfilment mechanisms (access, correction, erasure, grievance);
- For Significant Data Fiduciaries: review of Data Protection Impact Assessments, appointment of Data Protection Officer, and other requirements.

2.3 Scope Limitation

The audit provides a professional opinion based on information available during the audit period. It does not constitute legal advice, does not guarantee absolute regulatory compliance, and is subject to the inherent limitations of an audit conducted on a sampling basis.

3. Responsibilities of the Independent Data Auditor

3.1 Professional Standards

The Auditor shall at all times:

- Maintain independence in fact and in appearance throughout the engagement, refraining from any relationship that may impair objectivity;
- Adhere strictly to the AIDAI Code of Ethics, including principles of integrity, objectivity, confidentiality, professional competence, and due care;
- Exercise professional scepticism and apply risk-based audit methodology aligned with FDPPI and DGPSI frameworks;
- Obtain sufficient, relevant, and reliable audit evidence before forming opinions or reaching conclusions.

3.2 Reporting Obligations

The Auditor shall:

- Prepare and deliver all deliverables specified in Clause 7 and Annexure C within agreed timelines;
- Communicate material findings, control deficiencies, and significant risks to the Data Fiduciary's senior management promptly;
- Provide a draft report for management response prior to issuance of the Final Audit Report;
- Escalate to regulatory authorities where legally required or where there is evidence of material ongoing harm (see Clause 16).

3.3 Confidentiality and Data Security

The Auditor shall implement appropriate technical and organisational measures to protect all Confidential Information and personal data accessed during the audit, and shall not retain, copy, or process such data beyond what is strictly necessary for the audit purpose.

4. Responsibilities of the Data Fiduciary

The Data Fiduciary shall:

- Provide the Auditor with timely, unimpeded, and full access to all systems, networks, personnel, records, logs, policies, and documentation reasonably required for the audit;
- Designate a competent internal point of contact ("Audit Liaison") who shall facilitate the audit process and coordinate responses;
- Ensure the accuracy, completeness, and authenticity of all information and representations made to the Auditor;
- Maintain and demonstrate the operation of internal controls, compliance management systems, and data governance structures;
- Provide written management representations as and when requested by the Auditor;
- Respond to draft findings within the timelines specified in Annexure C;
- Implement agreed corrective and preventive actions within timelines agreed with the Auditor and report implementation status;
- Promptly notify the Auditor of any material changes to systems, processes, or organisational structure during the audit period that may affect the scope or findings.

5. Applicable Legal and Professional Framework

The audit shall be conducted with reference to the following, as applicable:

- Digital Personal Data Protection Act, 2023 and Rules made thereunder;
- Information Technology Act, 2000 as amended up to date.
- Applicable sectoral regulations (including RBI, SEBI, IRDAI, TRAI directives as relevant);
- DGPSI (Data Governance and Protection Standard of India) Framework developed by FDPPI;
- AIDAI Auditing Standards and Ethical Code;
- Any other applicable standard mutually agreed in Annexure B.

6. Audit Methodology and Limitations

6.1 Methodology

The audit shall employ a risk-based methodology and may include:

- Document review and policy gap analysis;
- Structured interviews with key personnel (technical, legal, compliance, and operational);
- Technical controls testing, vulnerability assessment review, and log analysis;
- Process walkthroughs and observation of operational controls;
- Sampling of personal data processing transactions, consent records, and data principal rights requests;
- Review of third-party processor contracts and compliance evidence.

6.2 Inherent Limitations

The Parties acknowledge that:

- An audit conducted on a sampling and risk-based basis cannot detect all instances of non-compliance or all deficiencies;
- The audit opinion reflects conditions as of the audit date and may not account for subsequent changes;
- The Auditor's findings are based on representations and evidence provided by the Data Fiduciary, which the Auditor cannot independently verify in all cases;
- The audit does not constitute a guarantee of regulatory immunity or legal compliance.

7. Audit Deliverables and Reporting

7.1 Deliverables

Subject to the scope and timelines in Annexure B and C, the Auditor shall provide:

- Audit Inception Report: confirming scope, methodology, and detailed work programme within 5 business days of commencement;
- Interim Findings Note (if applicable): summary of preliminary findings for management attention;
- Draft Audit Report: for management review and response, in the format prescribed in Annexure C;
- Final Audit Report: incorporating management responses, including the Auditor's opinion (unqualified, qualified, adverse, or disclaimer), findings, risk ratings, and recommendations;

- Management Letter: detailed communication of control weaknesses and improvement recommendations not included in the main report;
- Compliance Certificate or Non-Compliance Statement, as appropriate based on audit findings.
- Any other report as required under law.

7.2 Report Grading

Findings shall be risk-rated as Critical, High, Medium, or Low, with recommended remediation timelines. Critical and High findings shall be communicated verbally to senior management immediately upon identification, and documented in the interim note within 48 hours.

Where feasible, a Data Trust Score (DTS) may be provided to indicate the maturity status of the compliance in the organization as per the norms recommended by FDPPI.

7.3 Intellectual Property

All Audit Reports and deliverables are prepared for the exclusive use of the Data Fiduciary in connection with this engagement. The Data Fiduciary shall not reproduce, distribute, or publish audit deliverables without the Auditor's prior written consent, except as required by applicable law or regulatory obligation.

8. Fees, Expenses, and Payment Terms

8.1 Fees for this engagement shall be as set out in Annexure A (Fee Schedule), agreed upon at arms length and not contingent upon the findings or outcome of the audit.

8.2 The Fee Schedule shall distinguish between: (a) fixed professional fees; (b) reimbursable out-of-pocket expenses (subject to pre-approved limits); and (c) fees for any additional services agreed in writing.

8.3 Invoices shall be submitted as per the milestone schedule in Annexure A. Payment shall be made within 30 days of invoice date. Delayed payments shall attract interest at the rate of 1.5% per month from the due date.

8.4 Fees are exclusive of applicable taxes (including GST), which shall be charged additionally as per law.

8.5 The Auditor shall not receive any remuneration, benefit, or advantage from any third party in connection with this engagement.

9. Confidentiality and Data Protection

9.1 The Auditor undertakes to maintain strict confidentiality of all Confidential Information obtained during or in connection with this engagement and shall not disclose the same to any third party without prior written consent of the Data Fiduciary, except:

- Where disclosure is required by applicable law, court order, or regulatory requirement;
- Where disclosure is required to fulfil an ethical obligation under the AIDAI Code of Ethics;
- To professional advisers or sub-contractors of the Auditor who are bound by equivalent confidentiality obligations.

9.2 The Auditor shall process personal data encountered during the audit solely for the purposes of conducting the audit, in accordance with applicable data protection law, and shall not retain personal data beyond the period strictly necessary.

9.3 Confidentiality obligations shall survive termination of this Agreement for a period of five (5) years.

9.4 The Data Fiduciary acknowledges that the Auditor may be required to submit audit reports and working papers to AIDAI / FDPPI as part of quality review or regulatory oversight. The Data Fiduciary consents to such disclosure subject to AIDAI's own confidentiality obligations.

10. Ethical Compliance and Professional Conduct

10.1 The Auditor shall at all times comply with the AIDAI Code of Ethics, encompassing: integrity, objectivity, professional competence and due care, confidentiality, and professional behaviour.

10.2 The Auditor shall not accept gifts, hospitality, or benefits from the Data Fiduciary or any of its associated persons that could reasonably be perceived as impairing independence.

10.3 The Auditor shall not provide management consulting, legal advice, or other non-audit services to the Data Fiduciary in respect of matters under audit without adequate safeguards and written disclosure.

10.4 Any breach of this clause shall be grounds for immediate termination under Clause 18 and mandatory reporting to AIDAI.

11. Independence and Conflict of Interest

11.1 The Auditor represents and warrants that, as of the date of this Agreement, no circumstance exists that would impair independence. The Auditor shall conduct an independence assessment prior to commencing the audit and at each reporting milestone.

11.2 The Auditor shall immediately disclose in writing to the Data Fiduciary any actual, potential, or perceived conflict of interest that arises during the engagement, including without limitation:

- Financial interests in the Data Fiduciary or its competitors;
- Personal or familial relationships with key personnel;
- Prior consulting, legal, or other advisory engagements with the Data Fiduciary within the preceding three years;
- Simultaneous engagement with competing entities.

11.3 Upon disclosure of a conflict, the Parties shall in good faith assess whether the conflict can be mitigated or whether the Auditor must withdraw. The Auditor's prior reports shall not be automatically invalidated solely by reason of a subsequently disclosed conflict.

12. Liability and Indemnification

12.1 The Auditor's aggregate liability to the Data Fiduciary arising out of or in connection with this Agreement, whether in contract, tort (including negligence), breach of statutory duty, or otherwise, shall not exceed the total fees actually paid by the Data Fiduciary to the Auditor under this Agreement.

12.2 Neither Party shall be liable to the other for: (a) indirect, special, or consequential loss; (b) loss of profit, revenue, or business opportunity; (c) loss of goodwill or reputation; whether or not such losses were foreseeable or advised.

12.3 The liability limitations in Clauses 12.1 and 12.2 shall not apply to: (a) fraud or wilful misconduct; (b) death or personal injury caused by negligence; (c) any other liability that cannot be excluded or limited by law.

12.4 The Data Fiduciary shall indemnify the Auditor against any third-party claims, losses, or penalties arising from the Data Fiduciary's misrepresentation, failure to disclose material information, or non-implementation of critical recommendations.

12.5 The Auditor's liability for regulatory penalties or fines imposed on the Data Fiduciary is expressly excluded, as regulatory compliance remains the sole responsibility of the Data Fiduciary.

13. Dispute Resolution — Dual-Track Mechanism

13.1 Amicable Negotiation

Any dispute, controversy, or claim arising out of or in connection with this Agreement shall first be referred for resolution by senior representatives of both Parties through good faith negotiations within 30 days of written notice of the dispute.

13.2 Mediation

If negotiations are unsuccessful within the said 30 days, the dispute shall proceed to structured mediation facilitated by a mutually agreed mediator or through an institution recognised by FDPPI, within a further 30 days.

13.3 Classification of Disputes

Disputes shall be classified as follows to determine the applicable resolution track:

- Regulatory Disputes: disputes concerning compliance obligations, audit findings, or matters within the jurisdiction of the DPB or other regulatory authority;
- Contractual Disputes: disputes concerning fees, deliverables, timelines, liability, confidentiality, or other contractual rights and obligations.

13.4 Regulatory Track

Regulatory disputes shall be addressed in accordance with the DPDPA 2023 and may be referred to the Data Protection Board of India or other competent regulatory authority. The Parties shall cooperate fully with any such proceedings.

13.5 Contractual Track — Arbitration

Contractual disputes unresolved after mediation shall be finally resolved by binding arbitration under the Arbitration and Conciliation Act, 1996, with the following parameters:

- A sole arbitrator appointed by mutual agreement (or by the relevant institution in default);
- Seat and venue of arbitration: India (city to be specified in Annexure A);
- Language: English;
- Proceedings may be conducted through an online dispute resolution mechanism.

13.6 Parallel Proceedings

Regulatory and contractual tracks may proceed simultaneously and independently. A finding or order in one track shall not be binding in the other unless required by law.

13.7 Interim Relief

Nothing in this Clause shall prevent either Party from seeking urgent interim or injunctive relief from a court of competent jurisdiction to prevent irreparable harm, pending the outcome of the dispute resolution process.

14. Governing Law and Jurisdiction

14.1 This Agreement shall be governed by and construed in accordance with the laws of India.

14.2 Subject to the dispute resolution mechanism in Clause 13, the Parties submit to the exclusive jurisdiction of the courts at [City to be specified] for matters not subject to arbitration.

15. General Provisions

15.1 Entire Agreement

This Agreement, together with all Annexures, constitutes the entire agreement between the Parties with respect to the subject matter hereof and supersedes all prior negotiations, representations, warranties, and understandings.

15.2 Amendments

No amendment or variation of this Agreement shall be effective unless made in writing and signed by authorised representatives of both Parties.

15.3 Severability

If any provision of this Agreement is held invalid, illegal, or unenforceable by a court of competent jurisdiction, such provision shall be deemed modified to the minimum extent necessary to make it enforceable. All other provisions shall remain in full force.

15.4 Force Majeure

Neither Party shall be in breach or liable for delay or failure to perform obligations under this Agreement due to events beyond reasonable control, including acts of God, pandemic, war, civil unrest, or governmental action. The affected Party shall notify the other within 5 business days and use reasonable efforts to mitigate the impact. Obligations shall resume once the force majeure conditions cease.

15.5 No Waiver

Failure or delay by either Party to exercise any right or remedy under this Agreement shall not constitute a waiver of that right or remedy.

15.6 Assignment

Neither Party may assign or transfer its rights or obligations under this Agreement without the prior written consent of the other Party, except that the Auditor may engage qualified sub-contractors subject to written disclosure and the sub-contractors being bound by equivalent confidentiality and ethical obligations.

15.7 Notices

All notices under this Agreement shall be in writing and delivered by hand, registered post, or email with read receipt to the addresses specified in Annexure A. Notices shall be deemed received on the date of delivery or, for email, on the date of read receipt.

15.8 Counterparts

This Agreement may be executed in counterparts, each of which shall constitute an original, and together shall form one binding Agreement. Electronic signatures shall be valid.

16. Incident Escalation and Mandatory Reporting

16.1 Upon identifying or reasonably suspecting a Personal Data Breach or material security incident during the audit, the Auditor shall:

- Notify the Data Fiduciary verbally within 4 hours of identification;
- Provide written notification within 24 hours, including a preliminary description of the suspected breach;
- Preserve and document all relevant evidence encountered.

16.2 Upon receipt of such notification, the Data Fiduciary shall:

- Acknowledge receipt within 2 hours and initiate its incident response procedures immediately;
- Provide the Auditor with status updates at intervals not exceeding 24 hours until the incident is contained;
- Comply with its mandatory breach notification obligations to the DPB under Section 8(6) of the DPDPA 2023 within the prescribed timeframe.

16.3 The Auditor may independently escalate to the DPB or other competent authority, and shall be obligated to do so, where:

- There is evidence of a material ongoing risk to data principals;
- The Data Fiduciary demonstrates a pattern of non-cooperation, suppression of evidence, or failure to remediate critical findings within agreed timelines;
- The Auditor's ethical obligations under the AIDAI Code require such disclosure.

16.4 The Auditor shall not be liable for any consequences arising from a mandatory escalation made in good faith and on reasonable grounds.

17. Regulatory Cooperation and Disclosure

17.1 Both Parties shall cooperate fully and promptly with the DPB, AIDAI, FDPPI, and any other competent regulatory authority in connection with investigations, inspections, or inquiries relating to the subject matter of this Agreement.

17.2 The Auditor is authorised to disclose audit reports, working papers, or other information to AIDAI for quality assurance purposes or to regulatory authorities where required by law, ethical obligation, or under Clause 16.3.

17.3 The Data Fiduciary shall preserve all books of accounts, records, documentation, and evidence related to the audit subject matter for a minimum period of 7 years from the date of the Final Audit Report, or such longer period as required by applicable law.

17.4 Neither Party shall destroy, conceal, or tamper with any records that are or may be subject to regulatory scrutiny. Violation of this obligation shall constitute a material breach entitling the other Party to immediate termination.

18. Term and Termination

18.1 This Agreement shall come into force on the date of execution and shall remain in effect for the duration of the Audit Period specified in Annexure B, unless earlier terminated.

18.2 Either Party may terminate this Agreement for convenience upon 30 days' written notice. In such event, the Data Fiduciary shall pay fees for all work completed up to the termination date, and the Auditor shall deliver all work product completed to date.

18.3 Either Party may terminate immediately upon written notice in the event of:

- A material breach of this Agreement by the other Party, if unremedied within 15 days of written notice;
- Persistent non-cooperation or obstruction of the audit process by the Data Fiduciary;
- Breach of ethical obligations or loss of AIDAI empanelment by the Auditor;
- Insolvency, liquidation, or appointment of a receiver for either Party.

18.4 Upon termination, clauses relating to confidentiality (Clause 9), liability (Clause 12), dispute resolution (Clause 13), governing law (Clause 14), and regulatory cooperation (Clause 17) shall survive.

Execution

IN WITNESS WHEREOF, the Parties have executed this Agreement as of the date first written above.

FOR THE DATA FIDUCIARY

Signature: _____

Name: _____

Designation: _____

Organisation: _____

Date: _____

Place: _____

FOR THE INDEPENDENT DATA AUDITOR

Signature: _____

Name: _____

Designation: _____

AIDAI Reg. No.: _____

Date: _____

Place: _____

Annexures

Annexure A — Fee Schedule and Contact Details

Fee Component	Amount / Terms
Professional Fees (Fixed)	_____
Reimbursable Expenses (Cap)	_____
Milestone 1 — Inception Report	_____
Milestone 2 — Draft Report	_____
Milestone 3 — Final Report	_____
Payment Mode	_____
Invoice Address	_____
Arbitration Seat (Cl. 13.5)	_____
Notice Address — Data Fiduciary	_____
Notice Address — Auditor	_____

Annexure B — Audit Plan and Timeline

#	Audit Phase / Deliverable	Planned Start Date	Planned Completion
1	Engagement commencement & inception report	_____	_____
2	Data collection, document review & policy analysis	_____	_____
3	Technical controls testing & process walkthroughs	_____	_____
4	Interviews with key personnel	_____	_____
5	Interim findings communication (if applicable)	_____	_____
6	Draft Audit Report — issued for management response	_____	_____
7	Management response deadline	_____	_____
8	Final Audit Report & Management Letter	_____	_____
9	Certification / Non-Compliance Statement	_____	_____

Annexure C — Reporting Format and Standards

The Final Audit Report shall be structured as follows:

1. Executive Summary: including overall risk rating, number of findings by risk level, and key recommendations.
2. Scope and Methodology: detailed description of audit scope, standards applied, and limitations.

3. Background on the Data Fiduciary: organisational context relevant to data protection.
4. Detailed Findings: each finding to include — Finding Reference, Description, Risk Level (Critical / High / Medium / Low), Root Cause Analysis, Evidence Reference, Recommendation, Management Response, and Agreed Remediation Timeline.
5. Overall Compliance Opinion: unqualified, qualified, adverse, or disclaimer, with basis for the opinion.
6. Summary Findings Table: tabulated view of all findings.
7. Appendices: evidence index, personnel interviewed, documents reviewed.

Finding risk ratings shall be assigned as follows:

Critical	Immediate regulatory violation or significant ongoing risk of harm to data principals; requires remediation within 7 days.
High	Significant control weakness or non-compliance with material legal obligation; requires remediation within 30 days.
Medium	Moderate risk or partial non-compliance; requires remediation within 60 days.
Low	Minor gap, best practice recommendation, or observation; requires remediation within 90 days.