ACCREDION QUALIS

ScudoCyber Solutions Private Limited

Certification Body for Privacy & Information Security

DPDP STANDARD 2026

Digital Personal Data Protection Management System (DPMS)

Requirements, Certification Scheme & Implementation Guidance
Non-Accredited

First Edition | 2026

Based on: Digital Personal Data Protection Act, 2023 | DPDP Rules 2025
Aligned with: ISO/IEC 27701:2025 | ISO/IEC 27001:2022 | GDPR

AQ-DPDP-STD-2026-001

Foreword

The Digital Personal Data Protection Act, 2023 (DPDP Act) represents India's landmark legislative step towards establishing a robust, rights-based framework for the governance of personal data. Enacted by the Parliament of India, the Act creates binding obligations on organizations — designated as Data Fiduciaries — to process personal data of citizens in a lawful, fair, and transparent manner.

This Standard — DPDP Standard 2026 — has been developed by Accredion Qualis (AQ) as a structured management system framework that enables organizations to demonstrate compliance with the DPDP Act, 2023 and the DPDP Rules as notified. It is designed in the structure and language of internationally recognized management system standards such as ISO/IEC 27001:2022 and ISO/IEC 27701:2025, ensuring compatibility with existing Information Security and Privacy Management Systems.

The DPDP Standard 2026 is intended for use by:

- Data Fiduciaries of all sizes and sectors subject to the DPDP Act
- Significant Data Fiduciaries designated under Section 10 of the Act
- Data Processors processing personal data on behalf of Data Fiduciaries
- Government entities and regulatory bodies
- Certification bodies and auditors conducting DPDP compliance assessments

Accredion Qualis is committed to the responsible certification of organizations against this Standard, fostering trust, accountability, and the protection of the rights of Data Principals across India.

Accredion Qualis Certification Board
2026

Introduction

0.1 Purpose of this Standard

This Standard provides requirements for the establishment, implementation, maintenance, and continual improvement of a Digital Personal Data Protection Management System (DPMS). The DPMS is a systematic approach to managing personal data obligations under the Digital Personal Data Protection Act, 2023 and associated Rules.

NOTE

This Standard is designed to be compatible with other Accredion Qualis management system standards. Organizations certified to ISO/IEC 27001:2022 or ISO/IEC 27701:2025 may leverage their existing management system infrastructure to implement this Standard.

0.2 Relationship with the DPDP Act, 2023

The DPDP Act, 2023 establishes the legal basis for this Standard. The following key provisions of the Act are addressed by corresponding clauses in this Standard:

DPDP Act Section	Subject Matter	DPMS Clause
Section 4	Grounds for Processing	Clause 8.2
Section 6	Consent	Clause 8.2
Section 7	Notice	Clause 5.2
Section 11–14	Rights of Data Principals	Clause 8.3
Section 8	Obligations of Data Fiduciary	Clause 4–9
Section 9	Processing Children's Data	Clause 8.2.4
Section 10	Significant Data Fiduciary	Clause 4.3, 5.1
Section 17	Exemptions	Clause 4.1
Section 40	Data Breach	Clause 8.4

0.3 Process Approach

This Standard promotes the adoption of a process approach incorporating the Plan-Do-Check-Act (PDCA) cycle when developing, implementing, maintaining, and continually improving the DPMS. The PDCA cycle operates as follows:

Phase	Activity	Standard Clauses
PLAN	Establish DPMS scope, policies, risk assessment, and objectives	Clauses 4, 5, 6
DO	Implement controls, processes, and operational procedures	Clauses 7, 8
CHECK	Monitor, measure, audit, and review performance	Clause 9
ACT	Address nonconformities, implement improvements	Clause 10

0.4 Compatibility with Other Standards

Organizations may integrate the DPMS with their existing management systems. This Standard is harmonized with the High-Level Structure (HLS) used in ISO management system standards, enabling seamless integration with:

- ISO/IEC 27001:2022 – Information Security Management System
- ISO/IEC 27701:2025 – Privacy Information Management System
- ISO 9001:2015 – Quality Management System
- ISO 22301:2019 – Business Continuity Management System

Clause 1: Scope

This Standard specifies requirements for establishing, implementing, maintaining, and continually improving a Digital Personal Data Protection Management System (DPMS) within the context of an organization.

This Standard is applicable to any organization that:

1. Processes digital personal data of Data Principals in India, regardless of whether the processing takes place within India or outside India;
2. Processes digital personal data outside India in connection with any profiling of, or any activity of offering goods or services to, Data Principals within India;
3. Acts as a Data Fiduciary, Data Processor, or Significant Data Fiduciary as defined under the DPDP Act, 2023.

NOTE

The term 'personal data' in this Standard refers to 'Digital Personal Data' as defined under Section 2(t) of the DPDP Act, 2023, meaning data about or relating to a natural person who is directly or indirectly identifiable.

Clause 2: Normative References

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this Standard:

Reference	Title
DPDP Act, 2023	Digital Personal Data Protection Act, 2023
DPDP Rules, 2025	Digital Personal Data Protection Rules (as notified)
ISO/IEC 27001:2022	Information Security Management Systems – Requirements
ISO/IEC 27701:2025	Privacy Information Management System – Requirements and Guidance
ISO/IEC 29134:2017	Guidelines for Privacy Impact Assessment
ISO/IEC 29101:2018	Privacy Architecture Framework
GDPR (Ref)	General Data Protection Regulation (EU) 2016/679 (Reference Only)

Clause 3: Terms and Definitions

For the purposes of this Standard, the following terms and definitions apply:

3.1 Data Principal

The natural person to whom the personal data relates. Where the Data Principal is a child, the term includes the parents or lawful guardian of such child.

3.2 Data Fiduciary

Any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data.

3.3 Significant Data Fiduciary (SDF)

A Data Fiduciary notified as such by the Central Government under Section 10 of the DPDP Act, 2023 based on volume of data processed, sensitivity, or risk.

3.4 Data Processor

Any person who processes personal data on behalf of a Data Fiduciary.

3.5 Consent

Any freely given, specific, informed, and unambiguous indication of the Data Principal's wishes by a statement or clear affirmative action.

3.6 Consent Manager

A person registered with the Data Protection Board who enables Data Principals to give, manage, review, and withdraw consent.

3.7 Data Protection Board of India

The regulatory authority established under Section 18 of the DPDP Act, 2023.

3.8 Data Protection Officer (DPO)

A person designated by a Significant Data Fiduciary to ensure compliance with the DPDP Act.

3.9 Personal Data Breach

Any unauthorized processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data.

3.10 Processing

A wholly or partly automated operation or set of operations performed on digital personal data.

3.11 DPMS

Digital Personal Data Protection Management System established under this Standard.

3.12 DPIA

Data Protection Impact Assessment — a systematic process to identify and mitigate privacy risks associated with a processing activity.

3.13 RoPA

Records of Processing Activities — a register documenting all personal data processing activities within scope.

3.14 Grievance Officer

A person designated by a Data Fiduciary to handle complaints and grievances from Data Principals.

3.15 Data Localization

The requirement to store data within the geographical boundary of India.

Clause 4: Context of the Organization

4.1 Understanding the Organization and Its Context

The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its DPMS. The organization shall specifically determine and document:

4.1.1 Personal Data Landscape

- Categories of digital personal data processed (including sensitive personal data)
- Purposes for which personal data is collected and processed
- The role of the organization: Data Fiduciary, Data Processor, or both
- Identification of cross-border data flows and applicable transfer mechanisms

4.1.2 External Context

- Applicable provisions of the DPDP Act, 2023 and DPDP Rules
- Sector-specific regulations (RBI, IRDAI, SEBI, TRAI, MoHFW, etc.)
- Contractual obligations with Data Processors and third parties
- International regulatory requirements (GDPR, PDPA, etc.) where applicable

4.1.3 Internal Context

- Organizational structure, roles, and accountabilities
- Information technology and data management infrastructure
- Existing ISMS, BCMS, or other management system frameworks

Documented Evidence Required

Data Processing Landscape Register | Regulatory Applicability Matrix | Business Process Mapping with Data Flows

4.2 Understanding the Needs and Expectations of Data Principals

The organization shall determine the needs and expectations of Data Principals relevant to the DPMS, including:

- Right to access their personal data
- Right to correction and erasure of personal data
- Right to grievance redressal
- Right to withdraw consent at any time
- Right to nominate a nominee in the event of death or incapacity

Documented Evidence Required

Data Principal Rights Register | Stakeholder Expectation Matrix | Data Principal Communication Plan

4.3 Determining the Scope of the DPMS

The organization shall determine the boundaries and applicability of the DPMS. The scope shall include:

- All business units, departments, and functions processing personal data
- All applications, platforms, and systems handling personal data
- Geographic locations covered
- Third-party processors operating within the organizational boundary

Where an organization is notified as a Significant Data Fiduciary, the scope shall explicitly include compliance obligations under Section 10 of the DPDP Act, 2023, including:

- Appointment of a Data Protection Officer
- Periodic Data Protection Impact Assessments
- Algorithmic accountability measures
- Data Audits by independent auditors

Documented Evidence Required

DPMS Scope Statement (signed by top management) | Scope Boundary Diagram

4.4 Digital Personal Data Protection Management System

The organization shall establish, implement, maintain, and continually improve a DPMS, including the processes needed and their interactions, in accordance with the requirements of this Standard.

- Policies, procedures, and controls addressing each clause of this Standard
- Integration with existing ISMS and BCMS where applicable
- Full coverage of the personal data lifecycle: Collection → Processing → Storage → Sharing → Deletion

Documented Evidence Required

DPMS Manual | Process Interaction Diagram (Privacy Lifecycle) | Integrated Management System Map

Clause 5: Leadership

5.1 Leadership and Commitment

Top management shall demonstrate leadership and commitment with respect to the DPMS by:

4. Ensuring that the privacy policy and the privacy objectives are established and are compatible with the strategic direction of the organization
5. Ensuring the integration of DPMS requirements into the organization's business processes
6. Ensuring that the resources needed for the DPMS are available
7. Communicating the importance of effective personal data protection management
8. Ensuring that the DPMS achieves its intended outcome(s)
9. Directing persons to contribute to the effectiveness of the DPMS
10. For Significant Data Fiduciaries: Appointing a Data Protection Officer and ensuring the DPO reports directly to the board or equivalent governing body

Documented Evidence Required

Leadership Commitment Statement (Board Resolution or equivalent) | DPO Appointment Letter (for SDFs) | Privacy Governance Charter

5.2 Privacy Policy

Top management shall establish a privacy policy that:

- Is appropriate to the purpose of the organization
- Includes a commitment to satisfy applicable personal data protection requirements
- Includes a commitment to continual improvement of the DPMS

5.2.1 Public-Facing Privacy Notice

The organization shall publish and maintain a Privacy Notice accessible to Data Principals that includes, at minimum:

11. Name and contact details of the Data Fiduciary
12. Nature of personal data collected
13. Purpose and basis for processing
14. Rights available to Data Principals and the mechanism to exercise them
15. Details of the Grievance Officer including contact information
16. Information on cross-border data transfers, if applicable
17. Retention periods for personal data
18. Procedure for data breach notification to Data Principals

Documented Evidence Required

Public Privacy Notice (Website/App/Physical) | Internal Privacy Policy | Privacy Notice Review Log (annual minimum)

5.3 Organizational Roles, Responsibilities, and Authorities

Top management shall ensure that the responsibilities and authorities for roles relevant to the DPMS are assigned, communicated, and understood within the organization.

Role	Key Responsibilities	DPDP Act Reference
Top Management / Board	Overall accountability for DPMS; resource allocation; annual review	Section 8
Data Protection Officer (SDF only)	Monitor compliance; advise on DPIAs; single point of contact for DPBI; conduct audits	Section 10(2)(b)

Grievance Officer	Receive, acknowledge, and resolve Data Principal complaints within prescribed timelines	Section 13
Privacy/DPMS Team	Day-to-day implementation of DPMS; training; RoPA maintenance; consent management	Section 8
Data Processor Liaison	Manage DPAs; conduct due diligence on processors; monitor processor compliance	Section 8(2)
IT / Security Team	Implement technical safeguards; breach detection and reporting; access controls	Section 8(5)
Legal / Compliance	Monitor regulatory changes; legal review of consent notices; regulatory filings	Section 8

Documented Evidence Required

RACI Matrix for Privacy Roles | Organizational Structure Chart | Role-Specific Terms of Reference

Clause 6: Planning

6.1 Actions to Address Risks and Opportunities

When planning for the DPMS, the organization shall consider the issues and requirements referred to in Clauses 4.1 and 4.2, and determine the risks and opportunities that need to be addressed to:

- Ensure the DPMS can achieve its intended outcome(s)
- Prevent or reduce undesired effects
- Achieve continual improvement

6.1.1 Privacy Risk Assessment

The organization shall establish and maintain a privacy risk assessment process that:

19. Identifies privacy risks associated with personal data processing activities
20. Analyzes and evaluates the likelihood and impact of identified risks
21. Applies appropriate risk treatment measures

Privacy risk categories to be assessed shall include, at minimum:

- Unauthorized processing or disclosure of personal data
- Risks from profiling, automated decision-making, and algorithmic processing
- Data breach and cybersecurity risks
- Third-party and supply chain risks
- Risks from cross-border data transfers
- Risks specific to processing sensitive personal data (financial, health, biometric)
- Risks related to processing children's personal data

6.1.2 Data Protection Impact Assessment (DPIA)

The organization shall conduct a DPIA prior to commencing any processing activity that is likely to result in high risk to the rights of Data Principals. A DPIA is mandatory for:

- Large-scale processing of sensitive personal data
- Systematic profiling of Data Principals
- Use of new technologies with significant data processing implications
- Processing activities where the Significant Data Fiduciary designation triggers DPIA obligations

Documented Evidence Required

Privacy Risk Register (maintained and reviewed at least annually) | DPIA Reports (per high-risk processing activity) | Risk Treatment Plans

6.2 Privacy Objectives and Planning to Achieve Them

The organization shall establish privacy objectives at relevant functions and levels. Privacy objectives shall be:

- Consistent with the privacy policy
- Measurable (where practicable)
- Monitored and updated as required

Objective	Metric / KPI	Target
Valid Consent Captured	% of processing with documented valid consent	**100%**
Data Principal Rights (DSR) Resolution	SLA for acknowledgement / resolution	**3 / 30 days**

Breach Notification	Time to notify DPBI following breach discovery	**Within 72 hours**
Employee Privacy Training	% of staff completing annual DPDP training	**>= 95%**
Processor Compliance	% of processors with valid DPA in place	**100%**
Grievance Resolution	% grievances resolved within prescribed period	**>= 98%**
DPIA Completion	% of high-risk processing activities with current DPIA	**100%**

Documented Evidence Required

Privacy KPI Dashboard | Objective Setting Records | Management Review Minutes

6.3 Planning of Changes

When the organization determines the need for changes to the DPMS, the changes shall be carried out in a planned manner. Privacy implications shall be assessed for:

- Introduction of new systems, applications, or technologies processing personal data
- New data processing activities or expansion of existing activities
- Organizational restructuring affecting privacy roles and responsibilities
- Mergers, acquisitions, or outsourcing arrangements

Documented Evidence Required

Change Impact Assessment (Privacy Lens) | Privacy by Design Checklist for New Projects

Clause 7: Support

7.1 Resources

The organization shall determine and provide the resources needed for the establishment, implementation, maintenance, and continual improvement of the DPMS, including:

- Dedicated personnel with privacy expertise (DPO, Privacy Officer, Grievance Officer)
- Technology tools: Consent Management Platform, Data Subject Request (DSR) portal, DPIA tools, RoPA systems
- Financial resources for privacy program implementation and audit
- Access to legal expertise for DPDP Act compliance advisory

7.2 Competence

The organization shall ensure that persons doing work under the organization's control that affects its privacy performance are competent on the basis of appropriate education, training, or experience. The organization shall:

22. Determine the necessary competence of persons affecting privacy performance
23. Provide training or take other actions to acquire the necessary competence
24. Retain documented information as evidence of competence

Role	Required Competencies	Training Frequency
All Employees	DPDP Act basics, data handling procedures, breach reporting	Annual
DPO	DPDP Act, ISO 27701, DPIA methodology, regulatory liaison	Bi-annual + updates
Grievance Officer	DSR processes, escalation procedures, regulatory timelines	Annual
IT / Security Staff	Data security, breach detection, encryption, access control	Annual
Legal / Compliance	DPDP Act, sector regulations, contract law (DPAs)	As required
Management	Privacy governance, leadership obligations, risk oversight	Annual

Documented Evidence Required

Training Records | Competence Assessment Results | Training Needs Analysis

7.3 Awareness

Persons working under the organization's control shall be aware of:

- The privacy policy and their contribution to the effectiveness of the DPMS
- The implications of not conforming with DPMS requirements
- How to identify and report a potential personal data breach
- Consent requirements and restrictions on unauthorized processing
- Procedures for handling Data Principal rights requests

7.4 Communication

The organization shall determine the need for internal and external communications relevant to the DPMS, including:

Communication Type	Content	Audience	Frequency

Privacy Notice	Rights, purposes, contact details	Data Principals	Ongoing
Breach Notification	Nature, impact, remedial steps	DPBI + Principals	As required
Management Updates	KPIs, incidents, audit findings	Top Management	Quarterly
Regulatory Correspondence	Responses to DPBI notices, compliance reports	DPBI	As required
Processor Communication	DPA updates, audit results, incident alerts	Data Processors	Ongoing

7.5 Documented Information

The DPMS shall include documented information required by this Standard. The organization shall include the following core documents and records:

Document / Record	Type	Retention
DPMS Scope Statement	Controlled Document	Duration of DPMS
Privacy Policy & Notice	Controlled Document	Current + 3 years
Records of Processing Activities (RoPA)	Register	Duration + 5 years
Consent Logs	Record	Duration of consent + 5 years
Data Principal Rights Request Records	Record	5 years
Data Breach Register & Notifications	Record	5 years
DPIA Reports	Record	5 years post-activity
Training Records	Record	5 years
Data Processing Agreements	Controlled Document	Duration + 5 years
Internal Audit Reports	Record	3 years
Privacy Risk Register	Register	Current + 5 years

Clause 8: Operation

8.1 Operational Planning and Control

The organization shall plan, implement, control, monitor, and review the processes needed to meet requirements for the DPMS, by implementing the following principles throughout the personal data lifecycle:

Principle	Requirement	Control Measure
Collection Limitation	Collect only personal data that is necessary for the specified purpose	Data minimization review at point of collection
Purpose Limitation	Process personal data only for the purpose for which it was collected or for compatible purposes	Purpose registry and access controls
Storage Limitation	Retain personal data only for the duration necessary	Automated retention and deletion schedules
Accuracy	Ensure personal data is accurate and kept up to date	Data quality checks; correction mechanisms for Data Principals
Security Safeguards	Implement appropriate technical and organizational measures	Encryption, access control, vulnerability management
Accountability	Be responsible for compliance and able to demonstrate it	RoPA, audit trails, DPO oversight

8.2 Consent Management

8.2.1 Valid Consent Requirements

The organization shall ensure that consent obtained from Data Principals satisfies the following requirements under the DPDP Act, 2023:

- FREE – not conditional on service provision except where necessary
- SPECIFIC – linked to a clearly defined and limited purpose
- INFORMED – provided after adequate notice has been given
- UNAMBIGUOUS – evidenced by a clear affirmative act

8.2.2 Consent Notice

Prior to seeking consent, the organization shall provide the Data Principal with a notice in clear and plain language that includes:

25. Personal data sought to be collected and the purpose of processing
26. The manner in which consent may be withdrawn and the consequences thereof
27. The grievance redressal mechanism available to the Data Principal

8.2.3 Consent Withdrawal

The organization shall provide a mechanism for Data Principals to withdraw consent at any time, which shall be:

- As easy to exercise as the mechanism for giving consent
- Without any adverse effect on prior processing activities
- Processed within a reasonable time, not exceeding 30 days

8.2.4 Processing Children's Personal Data

Where the Data Principal is a child (below 18 years of age), the organization shall:

28. Obtain verifiable parental consent before processing the child's personal data
29. Refrain from processing that is likely to cause detrimental effect on the well-being of the child
30. Refrain from tracking, behavioral monitoring, or targeted advertising directed at children

Documented Evidence Required

Consent Logs (timestamped, per user, per purpose) | Consent UI/UX Screenshots | Consent Withdrawal Records | Age Verification Records

8.3 Data Principal Rights Handling

The organization shall establish documented procedures for receiving, acknowledging, and responding to Data Principal rights requests:

Right	Organizational Obligation	Response Timeline
Right to Access	Provide summary of personal data processed and processing activities	As prescribed by Rules
Right to Correction	Correct inaccurate or misleading personal data	As prescribed by Rules
Right to Erasure	Erase personal data upon withdrawal of consent or cessation of purpose	As prescribed by Rules
Right to Grievance Redressal	Acknowledge and resolve grievances; escalate to DPBI if unresolved	Within prescribed period
Right to Nominate	Allow nomination of person to exercise rights upon death or incapacity	Registration mechanism

Documented Evidence Required

DSR Tracking Log | Grievance Register | Response Records | Escalation Records to DPBI

8.4 Personal Data Breach Management

8.4.1 Breach Detection and Response

The organization shall maintain a documented breach management procedure that includes:

31. Detection and initial assessment of the breach
32. Containment and mitigation measures
33. Assessment of likely harm to Data Principals
34. Notification to the Data Protection Board of India in the form and manner prescribed
35. Notification to affected Data Principals where the breach is likely to cause harm

8.4.2 Breach Notification Requirements

Notification to the Data Protection Board of India shall be made promptly upon the occurrence of a personal data breach in such form and manner as may be prescribed. The notification shall contain at minimum:

- Nature and extent of the personal data breach
- Categories and approximate number of Data Principals affected
- Likely consequences of the breach
- Measures taken or proposed to address the breach

Documented Evidence Required

Personal Data Breach Register | Breach Notification Records (DPBI + Principals) | Post-Incident Review Reports

8.5 Third-Party and Processor Management

8.5.1 Data Processing Agreements

The organization shall ensure that each Data Processor processes personal data only on documented instructions from the Data Fiduciary. A written Data Processing Agreement (DPA) shall be in place with every Data Processor, containing at minimum:

- Scope and nature of processing authorized
- Instructions regarding security measures to be implemented
- Sub-processing restrictions and approval requirements
- Breach notification obligations and timelines
- Data deletion or return obligations upon contract termination
- Audit rights of the Data Fiduciary

8.5.2 Processor Due Diligence

The organization shall conduct due diligence on Data Processors prior to engagement and at regular intervals thereafter, assessing:

- Privacy and security certifications held by the processor
- Sub-processor arrangements and data residency
- Track record on data breaches and regulatory compliance

Documented Evidence Required

Data Processing Agreements (DPA) Register | Processor Due Diligence Records | Processor Audit Reports

8.6 Cross-Border Data Transfers

The organization shall not transfer personal data of Data Principals to any country or territory outside India, except to countries or territories as may be notified by the Central Government. The organization shall:

- Maintain an up-to-date list of notified countries to which transfers are permitted
- Ensure Data Processing Agreements with overseas processors specify compliance requirements
- Maintain records of all cross-border transfers
- Conduct transfer impact assessments where required

Documented Evidence Required

Cross-Border Transfer Register | Transfer Impact Assessments | Country Notification Monitoring Log

Clause 9: Performance Evaluation

9.1 Monitoring, Measurement, Analysis, and Evaluation

The organization shall determine what needs to be monitored and measured, the methods for monitoring, measurement, analysis, and evaluation, and when the results shall be analysed and evaluated.

Metric	Measurement Method	Frequency	Owner
DSR Request Volume & Resolution Rate	DSR Tracking System	Monthly	Grievance Officer
Consent Coverage Rate	Consent Management Platform	Monthly	Privacy Team
Breach Incidents (count, severity)	Breach Register	Monthly	IT / DPO
SLA Compliance for DSR	DSR Tracking System	Monthly	Grievance Officer
Training Completion Rate	LMS / HR System	Quarterly	HR / Privacy Team
Processor DPA Coverage	Vendor Register	Quarterly	Legal / Privacy
Open Privacy Risks (High/Critical)	Risk Register	Monthly	DPO
Regulatory Notices / Fines	Compliance Log	As required	Legal

9.2 Internal Audit

The organization shall conduct internal audits at planned intervals to provide information on whether the DPMS:

- Conforms to the organization's own requirements for the DPMS
- Conforms to the requirements of this Standard
- Is effectively implemented and maintained

9.2.1 Audit Program

The organization shall plan, establish, implement, and maintain an audit programme(s), including the frequency, methods, responsibilities, planning requirements, and reporting. The audit programme shall consider the importance of the processes concerned and the results of previous audits.

The audit programme shall cover, as a minimum:

- Consent management practices
- Data Principal rights handling procedures
- Data breach management capability
- Processor management and DPA compliance
- RoPA accuracy and completeness
- Technical security safeguards
- Training and competence records

Documented Evidence Required

Annual Audit Programme | Internal Audit Reports | Non-Conformity Logs | Corrective Action Plans

9.3 Management Review

Top management shall review the organization's DPMS at planned intervals to ensure its continuing suitability, adequacy, and effectiveness. The management review shall include consideration of:

- Status of actions from previous management reviews
- Changes in external and internal issues relevant to the DPMS
- Information on the DPMS performance including trends in: DSR requests, breaches, nonconformities, audit results, KPIs
- Opportunities for continual improvement
- Regulatory and legislative changes impacting the DPMS

Documented Evidence Required

Management Review Agenda | Management Review Minutes | Action Items Register

Clause 10: Improvement

10.1 Nonconformity and Corrective Action

When a nonconformity occurs, the organization shall:

36. React to the nonconformity and take action to control and correct it, dealing with the consequences
37. Evaluate the need for action to eliminate the causes of the nonconformity, so that it does not recur or occur elsewhere
38. Implement any action needed, review the effectiveness of any corrective action taken, and make changes to the DPMS if necessary

Nonconformities in the context of the DPMS include:

- Processing of personal data without valid consent or lawful basis
- Failure to respond to Data Principal rights requests within prescribed timelines
- Personal data breach not reported within required timeframe
- Processing by a Data Processor without a valid DPA
- Audit finding of non-compliance with this Standard or the DPDP Act

Documented Evidence Required

Nonconformity Register | Root Cause Analysis Records | Corrective Action Plans and Verification

10.2 Continual Improvement

The organization shall continually improve the suitability, adequacy, and effectiveness of the DPMS. Areas for continual improvement shall include:

- Privacy control effectiveness and automation
- Consent management technology and user experience
- Privacy governance maturity progression
- Integration of privacy by design and by default in product development
- Enhancement of Data Principal rights handling capabilities
- Advancement of privacy culture and awareness across the organization

Annex A: DPMS Control Framework (Normative)

This Annex provides the comprehensive control set for the DPMS. Organizations shall implement all applicable controls. Controls marked [SDF] are additionally mandatory for Significant Data Fiduciaries.

Ref.	Control Name	Control Requirement	Implementation Guidance
A.1	**Consent Control**	All processing of personal data shall be based on valid consent or another lawful basis identified in the DPDP Act	Deploy consent management platform; maintain consent logs; implement withdrawal mechanism
A.2	**Data Minimization**	Only personal data that is adequate, relevant, and limited to what is necessary in relation to the purpose shall be collected	Data mapping review; field-level necessity assessment; privacy by design reviews
A.3	**Purpose Limitation**	Personal data shall be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes	Purpose registry; access controls linked to purpose; change management process
A.4	**Storage Limitation**	Personal data shall not be retained beyond the period necessary for the specified purpose	Retention schedule; automated deletion or anonymization; storage review audits
A.5	**Security Safeguards**	Appropriate technical and organizational measures shall be implemented to protect personal data from unauthorized access, disclosure, alteration, or destruction	Encryption at rest and in transit; access controls; patch management; penetration testing
A.6	**Data Accuracy**	Reasonable steps shall be taken to ensure personal data is accurate and up to date	Data quality processes; correction mechanisms for Data Principals; periodic data cleansing
A.7	**Transparency**	Data Principals shall be provided with adequate notice about data processing in clear and plain language	Privacy notice reviews; readability testing; multilingual notices where appropriate
A.8	**Accountability**	The Data Fiduciary shall be responsible for complying with the DPDP Act and shall be able to demonstrate compliance	RoPA maintenance; DPO appointment [SDF]; privacy governance documentation
A.9	**Children's Data Protection [SDF]**	Enhanced safeguards shall be applied to personal data of children, including verifiable parental consent	Age verification; parental consent workflows; prohibition on targeted advertising to children
A.10	**Algorithmic Accountability [SDF]**	Significant Data Fiduciaries shall implement measures to ensure that algorithmic systems used for processing do not create risks to rights of Data Principals	Algorithm impact assessments; bias testing; human oversight mechanisms
A.11	**Breach Management**	Procedures for detecting, assessing, containing, and notifying personal data breaches shall be established and maintained	Breach response plan; DPBI notification process; Data Principal notification templates
A.12	**Processor Oversight**	Data Fiduciaries shall ensure Data Processors process personal data only as instructed and implement adequate safeguards	DPA template; processor onboarding checklist; periodic processor audits
A.13	**Cross-Border Transfer Controls**	Personal data shall be transferred outside India only to notified countries and with appropriate safeguards	Country notification monitoring; transfer impact assessment; contractual safeguards

A.14	**Grievance Redressal**	An accessible and effective mechanism for Data Principals to raise grievances shall be established and maintained	Designated Grievance Officer; tracking system; escalation to DPBI process
A.15	**Privacy by Design [SDF]**	Privacy shall be embedded into systems and products from the design stage	Privacy impact in project initiation; privacy-enhancing technologies; default privacy settings

Annex B: Records of Processing Activities (RoPA) Template (Informative)

Organizations shall maintain a RoPA. The following template specifies the minimum required fields:

Field	Description / Example
Processing Activity ID	Unique identifier (e.g., PA-2026-001)
Processing Activity Name	Customer onboarding | Employee payroll | Marketing analytics
Business Unit / System	CRM / HR System / Mobile App
Purpose of Processing	Fulfillment of service contract | Statutory obligation | Consent-based marketing
Lawful Basis	Consent | Legitimate Use | Compliance with law
Categories of Data Principals	Customers | Employees | Children | Visitors
Categories of Personal Data	Name, email, phone, financial data, health data, biometric data
Sensitive Personal Data?	Yes / No — if Yes, specify category
Data Sources	Directly from Data Principal | Third party | Publicly available
Recipients / Disclosures	Internal teams | Data Processors | Regulatory bodies
Cross-Border Transfers?	Yes / No — if Yes, specify country and safeguards
Retention Period	3 years | Duration of contract | 7 years (statutory)
Deletion / Anonymization Method	Secure deletion | Anonymization protocol | Archive policy
Technical Safeguards	Encryption (AES-256) | Role-based access control | Audit logs
DPIA Required?	Yes / No — if Yes, DPIA reference number
DPA in Place?	Yes / No — if Yes, DPA reference and processor name
Last Review Date	DD/MM/YYYY
RoPA Owner	Privacy Team | IT | Legal

Annex C: DPIA Template (Informative)

This template shall be used for all high-risk processing activities as identified in Clause 6.1.2.

Section 1: Processing Activity Description

Provide a detailed description of the processing activity, including its nature, scope, context, and purposes.

Section 2: Necessity and Proportionality Assessment

Assess whether the processing is necessary, relevant, and proportionate to the purpose pursued. Consider data minimization and purpose limitation.

Section 3: Risk Identification

Identify all potential risks to the rights and freedoms of Data Principals, including unauthorized access, discrimination, financial loss, reputational damage, or other significant harm.

Section 4: Risk Evaluation

Evaluate the likelihood and severity of each identified risk. Categorize risks as Low, Medium, High, or Critical.

Section 5: Risk Mitigation Measures

Describe the technical and organizational measures proposed to address identified risks. Reference applicable Annex A controls.

Section 6: Residual Risk Assessment

Assess the residual risk after proposed mitigation measures are applied. Document acceptance or escalation decision.

Section 7: DPO Consultation [SDF]

For Significant Data Fiduciaries, record the DPO's review and recommendations. Document any disagreements and their resolution.

Section 8: Approval and Sign-off

Record the names, roles, and dates of approval by relevant stakeholders (Business Owner, DPO, Legal Counsel, Top Management for high-risk activities).

Section 9: Review Schedule

Specify the date for the next DPIA review. Trigger conditions for early review (e.g., significant change in processing, new technology deployment).

Annex D: Personal Data Breach Register (Informative)

The following fields shall be captured for every personal data breach event:

Field	Description
Breach ID	Unique identifier (e.g., BR-2026-001)
Date & Time of Discovery	DD/MM/YYYY HH:MM
Date & Time of Occurrence (if known)	DD/MM/YYYY HH:MM or 'Unknown'
Discovered By	Name, role, and department
Nature of Breach	Unauthorized access | Accidental disclosure | Loss of device | Ransomware | Insider threat
Systems / Applications Affected	List all affected systems, applications, and databases
Categories of Personal Data Affected	Name, financial, health, biometric, contact details, etc.
Number of Data Principals Affected (Approx.)	Numeric estimate or range
Sensitive Personal Data Involved?	Yes / No — if Yes, specify categories
Likely Harm to Data Principals	Identity theft | Financial loss | Discrimination | Reputational damage | No harm
Severity Assessment	Low / Medium / High / Critical
Containment Measures Taken	Describe immediate actions to contain the breach
DPBI Notification Date	DD/MM/YYYY HH:MM — or 'Not Required' with justification
Data Principal Notification Date	DD/MM/YYYY — or 'Not Required' with justification
Root Cause	Description of root cause identified through investigation
Corrective Actions Implemented	Technical and organizational measures implemented post-breach
Lessons Learned	Key lessons and process improvements arising from the breach
Case Closure Date	DD/MM/YYYY
Closed By (DPO / Privacy Officer)	Name and designation

Annex E: AQ Certification Scheme for DPDP Standard 2026

This Annex establishes the Accredion Qualis (AQ) Certification Scheme for the DPDP Standard 2026. The scheme defines the requirements, process, and obligations for organizations seeking third-party certification of their Digital Personal Data Protection Management System (DPMS).

Legal Basis

The AQ Certification Scheme is designed to facilitate organizations in demonstrating compliance with the Digital Personal Data Protection Act, 2023 and associated Rules. Certification does not constitute legal compliance advice and does not substitute the organization's own compliance obligations.

E.1 Certification Scheme Overview

The AQ Certification Scheme for DPDP Standard 2026 follows a three-year certification cycle consisting of:

Year	Audit Type	Description
Year 1	**Initial Certification Audit**	Stage 1 (Documentation Review) + Stage 2 (On-site Assessment). Successful completion leads to issuance of DPDP Standard 2026 Certificate.
Year 2	**First Surveillance Audit**	Verification that the DPMS remains implemented, effective, and continually improved. Scope covers mandatory audit areas plus findings from Year 1.
Year 3	**Second Surveillance Audit + Recertification Decision**	Full surveillance audit. At end of Year 3, recertification decision is made based on overall audit programme. New 3-year cycle begins.

E.2 Year 1 — Initial Certification Audit

E.2.1 Prerequisites for Initial Certification

Before applying for initial certification, the organization shall have:

- Implemented the DPMS in accordance with all applicable clauses of this Standard
- Operated the DPMS for a minimum of three (3) months prior to the Stage 2 audit
- Completed at least one full internal audit cycle against this Standard
- Conducted at least one management review of the DPMS
- Established and documented a Privacy Risk Register and current RoPA
- Appointed a Grievance Officer and, where applicable (SDF), a Data Protection Officer

E.2.2 Stage 1 — Documentation Review (Off-site)

The Stage 1 audit is a documentation review conducted off-site (or at the organization's premises) to:

39. Review the organization's documented information against the requirements of this Standard
40. Evaluate the organization's understanding of the Standard, particularly key requirements
41. Review the DPMS scope, policy, RoPA, Privacy Risk Register, and management review records
42. Identify any significant gaps that would indicate the organization is not ready for the Stage 2 audit

Stage 1 Document Review Area	Minimum Document Package Required
Context & Scope	DPMS Scope Statement, Regulatory Applicability Matrix, Data Processing Landscape Register
Leadership	Leadership Commitment Statement, Privacy Policy, Org Chart with privacy roles, DPO Appointment [SDF]

Planning	Privacy Risk Register (current), DPIA Reports (if applicable), Privacy Objectives & KPIs
Support	Training Records, Competence Evidence, Communication Procedures, Documented Information List
Operation	RoPA, Consent Management Procedures, DSR Procedures, Breach Management Procedure, DPA Register
Performance Evaluation	Internal Audit Reports, Non-Conformity Log, Management Review Minutes

Following Stage 1, AQ shall issue a Stage 1 Audit Report and a Stage 1 Findings Letter identifying any areas for improvement prior to Stage 2. A minimum of 30 days shall be provided to the organization to address Stage 1 findings.

E.2.3 Stage 2 — Certification Audit (On-site)

The Stage 2 audit is an on-site assessment to evaluate the implementation, effectiveness, and operation of the DPMS. The audit shall include:

Audit Area	Audit Activities	Evidence Sampled
Clause 4 – Context	Review context analysis, scope boundaries, regulatory mapping	Scope document, regulatory matrix, interviews
Clause 5 – Leadership	Interview top management, review governance structure, DPO engagement [SDF]	Leadership commitment statement, DPO appointment
Clause 6 – Planning	Review risk register, DPIA reports, objective setting	Risk register, DPIA, KPI reports
Clause 7 – Support	Sample training records, awareness sessions, communication logs	Training records, LMS reports
Clause 8.2 – Consent	Test consent collection mechanisms, review consent logs	Consent logs, UI screenshots, withdrawal samples
Clause 8.3 – DSR Handling	Review DSR workflow, sample completed requests, check timelines	DSR log, response records, escalation records
Clause 8.4 – Breaches	Review breach procedure, test with scenarios, check breach register	Breach register, notification records
Clause 8.5 – Processors	Sample DPAs, review processor due diligence records	DPA register, vendor assessments
Clause 8.6 – Cross-Border	Verify transfer register and country notification compliance	Transfer register, DPAs with overseas processors
Clause 9 – Evaluation	Review audit reports, management review minutes, KPI dashboard	Audit programme, MR minutes, KPI data
Clause 10 – Improvement	Verify corrective actions from internal audits are closed effectively	NCR log, CA plans, verification records
Annex A Controls	Sample implementation of applicable controls across Annex A	Control evidence, technical configurations

E.2.4 Audit Findings Classification

Classification	Definition	Impact on Certification
Major Nonconformity	Absence of a required control or systemic failure to implement a clause requirement; or multiple related minor nonconformities	Certification not granted until resolved and verified

Minor Nonconformity	Isolated lapse in implementation or isolated gap against a requirement	Certificate issued with requirement to resolve within 90 days
Observation / OFI	Opportunity for improvement; not a nonconformity against the Standard	Noted in audit report; no mandatory action

E.2.5 Certification Decision and Certificate Issuance

Following the Stage 2 audit and satisfactory resolution of any major nonconformities, AQ's Certification Decision Panel shall review the audit report and make the certification decision. Upon a positive decision:

- The organization is issued a DPDP Standard 2026 Certificate valid for three (3) years from the date of certification decision
- The certificate specifies the scope of certification, applicable clauses, and the certification date
- The organization is listed on the AQ Public Certification Register
- The organization may use the AQ DPDP Certified mark subject to AQ Certification Mark Policy

E.3 Year 2 — First Surveillance Audit

E.3.1 Purpose and Scope

The first surveillance audit shall be conducted within twelve (12) months of the initial certification decision (no later than 12 months after Stage 2 completion). The purpose of the surveillance audit is to:

- Confirm continued conformance with the requirements of this Standard
- Verify that identified nonconformities from Year 1 have been effectively resolved
- Assess the ongoing effectiveness of the DPMS and evidence of continual improvement
- Review any significant changes to the organization, scope, or personal data processing activities

E.3.2 Mandatory Surveillance Audit Areas — Year 2

The following areas are mandatory in every surveillance audit:

#	Mandatory Area	Rationale
1	**Internal Audit Programme & Results**	Evidence of ongoing self-assessment since Year 1
2	**Management Review Conduct & Minutes**	Evidence of top management oversight
3	**DPMS Changes & Change Management**	Any new processing, systems, or structural changes impacting the DPMS
4	**Corrective Actions from Year 1**	Closure and effectiveness verification of prior findings
5	**Consent Management (sample)**	Continued validity and completeness of consent records
6	**DSR Handling (sample)**	Compliance with response timelines and procedures
7	**Breach Register Review**	Any breaches since Year 1 and adequacy of response
8	**Privacy Objectives & KPI Performance**	Evidence of measurement and achievement against objectives
9	**Training Records (sample)**	Currency of employee privacy competence
10	**Processor DPA Currency**	Validity and completeness of DPAs with active processors

Additional audit areas may be selected by the AQ Lead Auditor based on: prior nonconformities and observations; risk profile of the organization; any complaints received; regulatory developments; and significant changes to scope.

E.3.3 Surveillance Audit Duration

The duration of the surveillance audit shall be not less than 50% of the initial Stage 2 audit duration. Exact audit days shall be determined by AQ based on the organization's scope, size, and complexity.

E.3.4 Outcome of Year 2 Surveillance Audit

Following the Year 2 surveillance audit:

- If no major nonconformities are found, the certificate remains valid
- If a major nonconformity is found, the organization shall provide a corrective action plan within 30 days, with implementation verified by a follow-up audit or documented evidence review within 90 days
- If major nonconformities are not resolved, AQ may suspend or withdraw the certificate

E.4 Year 3 — Second Surveillance Audit and Recertification

E.4.1 Second Surveillance Audit

The second surveillance audit shall be conducted within twelve (12) months of the first surveillance audit (i.e., within 24 months of initial certification). The scope of the Year 3 surveillance audit shall be at least as comprehensive as the Year 2 surveillance audit, with particular attention to:

- Long-term effectiveness and maturity of the DPMS
- Evidence of continual improvement over the three-year certification cycle
- Resolution and non-recurrence of issues identified in Year 1 and Year 2
- Emerging regulatory requirements and their integration into the DPMS

E.4.2 Recertification Decision

Following the Year 3 surveillance audit, AQ's Certification Decision Panel shall conduct a recertification review considering the full audit programme over the three-year cycle. The recertification decision shall assess:

43. The results of the Year 3 surveillance audit
44. Complaints received and their resolution during the certification cycle
45. The effectiveness of the DPMS over the three-year period
46. Evidence of continual improvement and maturity progression

Upon a positive recertification decision:

- A new DPDP Standard 2026 Certificate is issued for a further three (3) years
- A new three-year surveillance cycle commences

E.5 Certification Cycle Summary

Milestone	Activity	Timing	Audit Scope	Outcome
Pre-Certification	Application & Contract	T-0	Application review; scoping agreement	AQ quotation and audit plan issued
T + 1-4 weeks	Stage 1 Audit	T + 1 month	Documentation review	Stage 1 report; readiness decision
T + 6-12 weeks	Stage 2 Audit	T + 2-3 months	Full on-site implementation audit	Audit report; certification decision
T + 2-3 months	Certificate Issued	Post-Stage 2	Certification decision panel review	3-year certificate; AQ register listing
T + 12 months	Year 2 Surveillance	Year 1 anniversary	Mandatory areas + risk-based sampling	Continued certification (or NCR action)

T + 24 months	Year 3 Surveillance	Year 2 anniversary	Full surveillance; recertification review	Continued certification or corrective action
T + 36 months	Recertification	End of cycle	Full recertification review	New 3-year certificate issued

E.6 Special Audits

AQ may conduct special audits in the following circumstances:

- Extension of scope requested by the certified organization
- Transfer of certification from another certification body
- Following a significant data breach reportable to the DPBI
- Following receipt of a material complaint against the certified organization
- Following notification of the organization as a Significant Data Fiduciary
- Short-notice or unannounced audits where AQ determines a risk to certification integrity

E.7 Suspension and Withdrawal of Certification

Action	Grounds	Process
Suspension	Major nonconformity unresolved within agreed timeframe; failure to pay fees; misuse of certification mark; failure to permit surveillance audit	AQ notifies organization; suspension period of up to 6 months; certificate cannot be claimed during suspension
Withdrawal	Major nonconformity unresolved after suspension; voluntary surrender; evidence of fraud or misrepresentation; regulatory finding of material non-compliance with DPDP Act	AQ notifies organization and DPBI if relevant; organization removed from AQ public register; certificate recalled

E.8 Appeals and Complaints

Any organization dissatisfied with an AQ certification decision may submit a formal appeal to the AQ Appeals Committee within thirty (30) days of the notification of the decision. The Appeals Committee shall comprise persons not involved in the original certification decision.

Complaints regarding certified organizations may be submitted by any Data Principal, regulatory body, or other interested party to AQ. AQ shall investigate all material complaints and may initiate a special audit as a result.

E.9 Use of the AQ Certification Mark

Certified organizations are granted a non-exclusive, non-transferable license to use the AQ DPDP Certified Mark subject to the following conditions:

- The mark shall only be used in relation to activities within the certified scope
- The mark shall not be used in a manner that implies product certification or regulatory approval
- The mark shall not be altered, modified, or combined with other marks
- Use of the mark is immediately suspended upon suspension of certification
- Organizations shall include the certification scope and registration number when using the mark

E.10 Auditor Qualification Requirements

AQ Lead Auditors conducting DPDP Standard 2026 audits shall hold:

- A relevant tertiary qualification in law, information technology, or a related field
- Certification as a Lead Auditor for ISO/IEC 27001 or ISO/IEC 27701
- Demonstrated knowledge of the DPDP Act, 2023 and DPDP Rules
- A minimum of three (3) years of relevant professional experience in privacy, information security, or compliance auditing
- Completion of the AQ DPDP Lead Auditor Training Programme

Bibliography

The following documents, while not normative references, provide useful context and guidance for implementation of this Standard:

- Ministry of Electronics and Information Technology (MeitY), Digital Personal Data Protection Act, 2023
- Ministry of Electronics and Information Technology (MeitY), DPDP Rules, 2025
- ISO/IEC 27001:2022, Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems
- ISO/IEC 27701:2025, Security Techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management
- ISO/IEC 29134:2017, Information Technology — Security Techniques — Guidelines for Privacy Impact Assessment
- ISO/IEC 29101:2018, Information Technology — Security Techniques — Privacy Architecture Framework
- ISO/IEC 27018:2019, Code of Practice for Protection of Personally Identifiable Information in Public Clouds
- NIST Privacy Framework Version 1.0, National Institute of Standards and Technology, 2020
- Data Protection Board of India — Guidance Documents (as published from time to time)
- European Data Protection Board (EDPB) — Guidelines (for comparative reference)

DPDP Standard 2026 — Digital Personal Data Protection Management System

Published by Accredion Qualis | Document Reference: AQ-DPDP-STD-2026-001 | First Edition, 2026