DIGITAL PERSONAL DATA PROTECTION ACT 2023 & RULES 2025

COMPREHENSIVE COMPLIANCE AUDIT REPORT

AUDIT DETAILS			
Client / Entity Name	_____	**Industry / Sector**	
Review Date	_____	_____	
Lead Reviewer	_____	**Designation**	
Reviewer Contact	_____	Bar Enrolment No.	
Audit Scope	Full DPDP Act 2023 & Rules 2025 Compliance	**Version**	
Report Date	_____	1.0	

OVERALL COMPLIANCE ASSESSMENT	
TOTAL SCORE _____ / 100	**COMPLIANCE RATING** _____

Prepared pursuant to the Digital Personal Data Protection Act, 2023 (No. 22 of 2023) and the Digital Personal Data Protection Rules, 2025 (notified 14 November 2025)

Important Notice & Scope

DISCLAIMER

This report is a professional legal compliance audit tool prepared under the Digital Personal Data Protection Act, 2023 and DPDP Rules, 2025. It is prepared by a licensed advocate and constitutes legal work product. It does not constitute a final legal opinion and should be read alongside the full text of the Act and Rules.

Applicable Law References:

- Digital Personal Data Protection Act, 2023 (No. 22 of 2023) — Assented: 11 August 2023
- Digital Personal Data Protection Rules, 2025 — Notified: 14 November 2025
- Information Technology Act, 2000 (as amended by DPDP Act, Section 44)
- Right to Information Act, 2005 (as amended by DPDP Act, Section 44(3))
- K.S. Puttaswamy vs Union of India, (2017) 10 SCC 1 — Privacy as Fundamental Right

Key Statutory Timelines (DPDP Rules 2025)

Obligation	Timeline	Statutory Reference
Respond to Data Principal rights requests (access, correction, erasure, updating)	**90 days**	DPDP Rules 2025, Rule on Section 11-12
Respond to Data Principal grievances	**30 days**	DPDP Rules 2025 (Sec 13(2))
Notify affected individuals of personal data breach	**Without delay (immediately)**	Sec 8(6) + DPDP Rules 2025
Submit detailed breach report to DPBI	**Within 72 hours of first intimation**	DPDP Rules 2025
Phased compliance period for organisations	**18 months from Rules notification**	DPDP Rules 2025 (i.e., by May 2027)
Appeal period against DPBI order	**60 days from receipt of order**	Sec 29(2) DPDP Act
TDSAT to dispose appeals (target)	**6 months from filing**	Sec 29(6) DPDP Act
Data erasure upon consent withdrawal	**Within reasonable time**	Sec 8(6) DPDP Act
Data deemed purpose-served (auto-delete trigger)	**As prescribed per DF category**	Sec 8(8) DPDP Act
DPO appointed by SDF — must be India-based	**Ongoing obligation**	Sec 10(2)(a) DPDP Act

Section 1: Data Inventory & Mapping [10 Points]

1. DATA INVENTORY & MAPPING					
#	Requirement	Yes	No	N/A	Section Ref / Evidence
1.1	Complete inventory of all personal data collected by the organisation exists and is up-to-date	☐	☐	☐	Sec 8(1), 8(4)
1.2	Data flow map documented: collection → processing → storage → sharing → deletion — covering all data categories	☐	☐	☐	Sec 8(5)
1.3	All data storage locations identified: on-premise servers, cloud (AWS/Azure/GCP), third-party SaaS, employee devices	☐	☐	☐	Sec 8(4)
1.4	Retention periods defined for each data category in accordance with Sec 8(7) and applicable sector laws	☐	☐	☐	Sec 8(7)-(8)
1.5	Data classification system operational: sensitive personal data identified separately (financial, health, biometric, children's)	☐	☐	☐	Sec 9, Rules 2025
1.6	Register of all processing activities maintained (purpose, legal basis, data type, processor, retention)	☐	☐	☐	Sec 8(1)
1.7	All third-party Data Processors identified, documented, and mapped to the data they receive	☐	☐	☐	Sec 8(2), 2(k)
1.8	Data Access Matrix (RBAC) exists — defines who within the organisation can access which personal data	☐	☐	☐	Sec 8(4)-(5)
1.9	Regular data inventory audits scheduled and conducted (minimum annually)	☐	☐	☐	Sec 10(2)(c)(ii) for SDF
1.10	Shadow IT / undocumented data processing streams identified, assessed, and either regularised or discontinued	☐	☐	☐	Sec 8(1)
Section Score: _____ / ___ | Critical Gaps Noted: _____					

Section 2: Legal Basis for Processing [10 Points]

2. LEGAL BASIS FOR PROCESSING (SECTION 4, 7 — DPDP ACT 2023)					
#	Requirement	Yes	No	N/A	Section Ref / Evidence
2.1	Valid legal basis (Consent OR Certain Legitimate Use under Sec 7) identified and documented for EVERY processing activity	☐	☐	☐	Sec 4(1)
2.2	Consent obtained where required; organisation NOT relying on 'legitimate use' for activities that actually require consent	☐	☐	☐	Sec 4(1)(a)
2.3	Where Sec 7 Legitimate Use is relied upon, the specific sub-clause (a)–(i) is documented for each processing activity	☐	☐	☐	Sec 7(a)-(i)

2.4	Purpose Limitation observed: data not processed for any purpose beyond what is stated in the notice to Data Principal	☐	☐	☐	Sec 6(1), 2(za)
2.5	Data Minimisation principle followed: only minimum data necessary for specified purpose is collected (Sec 6(1))	☐	☐	☐	Sec 6(1)
2.6	'Just-in-case' data collection eliminated: no data collected without a current, documented, lawful processing purpose	☐	☐	☐	Sec 6(1), 8(4)
2.7	Legal basis reviewed and re-documented whenever a new processing activity or product feature is introduced	☐	☐	☐	Sec 8(4)
2.8	Legal basis clearly stated in Privacy Notice / consent request made available to Data Principals	☐	☐	☐	Sec 5(1)
2.9	Processing under Sec 7(b) (State benefits) follows Central Government notified standards; applicable only to State/instrumentalities	☐	☐	☐	Sec 7(b)
2.10	Processing for research/archiving/statistics (if applicable) does not use data to make decisions specific to any Data Principal	☐	☐	☐	Sec 17(2)(b)
Section Score: _____ / ___ | Critical Gaps Noted: _____					

Section 3: Notice Requirements — DPDP Specific [10 Points]

NOTE: DPDP Act Sections 5 & 6(3) mandate specific notice requirements not present in most international privacy frameworks. This section is unique to DPDP compliance.

3. NOTICE REQUIREMENTS — SECTION 5 & 6(3), DPDP ACT 2023

#	Requirement	Yes	No	N/A	Section Ref / Evidence
3.1	Notice accompanies or precedes every consent request — no consent solicited without prior/simultaneous notice [Sec 5(1)]	☐	☐	☐	Sec 5(1)
3.2	Notice specifies: (i) personal data to be processed, (ii) exact purpose, (iii) how to exercise rights under Sec 6(4) & 13	☐	☐	☐	Sec 5(1)(i)-(iii)
3.3	Notice informs Data Principal of the manner to make a complaint to the Data Protection Board of India	☐	☐	☐	Sec 5(1)(iii)
3.4	Notice available in ENGLISH and in any of the 22 languages listed in the 8th Schedule to the Constitution of India [Sec 5(3)]	☐	☐	☐	Sec 5(3) & 6(3)
3.5	Notice written in clear, plain, simple language — not in legal jargon; accessible to a layperson	☐	☐	☐	SARAL Principle, Rules 2025
3.6	Where consent was obtained BEFORE commencement of the Act, retrospective notice issued to existing users 'as soon as reasonably practicable' [Sec 5(2)]	☐	☐	☐	Sec 5(2)
3.7	Consent request (in addition to notice) separately available in English or any 8th Schedule language at Data Principal's option [Sec 6(3)]	☐	☐	☐	Sec 6(3)
3.8	Consent request/notice contains DPO contact details or other authorised person's details where applicable [Sec 6(3)]	☐	☐	☐	Sec 6(3)
3.9	Separate, standalone notice issued for each distinct processing purpose — not one omnibus 'terms of service' covering all purposes	☐	☐	☐	Rules 2025, Sec 6(1)
3.10	Notice accessible via voice/audio format where relevant (AI-driven or voice interfaces), reflecting DPDP Rules 2025 future-proofing requirement	☐	☐	☐	Rules 2025

Section Score: _____ / ___ | Critical Gaps Noted: _____

Section 4: Consent Management [15 Points]

4A. CONSENT COLLECTION — SECTION 6, DPDP ACT 2023

#	Requirement	Yes	No	N/A	Section Ref / Evidence
4.1	Consent is FREE — not bundled, not coerced, not a pre-condition to a service where processing is not necessary for that service	☐	☐	☐	Sec 6(1)

4.2	Consent is SPECIFIC — separate consent sought for each distinct processing purpose; no omnibus/blanket consent	☐	☐	☐	Sec 6(1)
4.3	Consent is INFORMED — Privacy Notice provided before consent; Data Principal made fully aware of processing activities	☐	☐	☐	Sec 6(1)
4.4	Consent is UNCONDITIONAL — no conditions attached that would undermine Data Principal's free choice	☐	☐	☐	Sec 6(1)
4.5	Consent is UNAMBIGUOUS with CLEAR AFFIRMATIVE ACTION — pre-ticked boxes, silence, inaction do NOT constitute valid consent	☐	☐	☐	Sec 6(1)
4.6	No clause in consent waives Data Principal's right to file a complaint with the DPBI [Sec 6(2) makes such waiver invalid]	☐	☐	☐	Sec 6(2)
4.7	Verifiable PARENTAL CONSENT obtained for all users under 18 years of age before any processing of their personal data	☐	☐	☐	Sec 9(1)

Section Score: _____ / ___ | Critical Gaps Noted: _____

4B. CONSENT RECORDS — SECTION 6(10)

#	Requirement	Yes	No	N/A	Section Ref / Evidence
4.8	Consent records maintained with: timestamp, identity of Data Principal, scope of consent, version of notice shown	☐	☐	☐	Sec 6(10)
4.9	Organisation can demonstrate (burden of proof on Data Fiduciary) that notice was given and consent obtained [Sec 6(10)]	☐	☐	☐	Sec 6(10)
4.10	Consent records stored securely and accessible for producing evidence in Board proceedings	☐	☐	☐	Sec 6(10), 28(7)

Section Score: _____ / ___ | Critical Gaps Noted: _____

4C. CONSENT WITHDRAWAL — SECTION 6(4)-(6)

#	Requirement	Yes	No	N/A	Section Ref / Evidence
4.11	Easy, single-step mechanism to WITHDRAW consent available — at least as easy as the mechanism used to give consent	☐	☐	☐	Sec 6(4)
4.12	No dark patterns: consent withdrawal not buried in settings, not requiring multiple steps disproportionate to giving consent	☐	☐	☐	Sec 6(4)
4.13	Processing stops within reasonable time upon consent withdrawal; Data Processors also instructed to cease [Sec 6(6)]	☐	☐	☐	Sec 6(6)
4.14	Data Principal's existing rights/orders honoured post-withdrawal (e.g., delivery of goods already ordered and paid for) [Sec 6(5)]	☐	☐	☐	Sec 6(5)

4.15	Consent Manager (if used) is registered with the DPBI and meets all prescribed technical/operational/financial conditions [Sec 6(9)]	☐	☐	☐	Sec 6(7)-(9)
Section Score: _____ / ___ | Critical Gaps Noted: _____					

Section 5: Legitimate Uses Assessment [5 Points]

5. CERTAIN LEGITIMATE USES — SECTION 7, DPDP ACT 2023					
#	Requirement	Yes	No	N/A	Section Ref / Evidence
5.1	Where processing is based on Sec 7(a) [voluntary provision], the specific purpose for which data was voluntarily given is documented and processing stays limited to that purpose	☐	☐	☐	Sec 7(a)
5.2	Where Sec 7(b) applies [State benefits/subsidies], only State/instrumentalities process data; applicable Central Govt. notified standards followed	☐	☐	☐	Sec 7(b)
5.3	Medical emergency / epidemic / disaster processing [Sec 7(f)-(h)] is limited in scope and duration to the specific emergency; no data retained post-emergency without fresh legal basis	☐	☐	☐	Sec 7(f)-(h)
5.4	Employment-related processing [Sec 7(i)] limited to documented employer protection purposes (trade secrets, corporate espionage prevention); employees made aware	☐	☐	☐	Sec 7(i)
5.5	Organisation does NOT use a Sec 7 Legitimate Use as a blanket substitute for obtaining consent where consent is the appropriate legal basis	☐	☐	☐	Sec 4(1), 7
Section Score: _____ / ___ | Critical Gaps Noted: _____					

Section 6: Individual Rights (Data Principal Rights) [12 Points]

6A. RIGHT TO ACCESS INFORMATION — SECTION 11					
#	Requirement	Yes	No	N/A	Section Ref / Evidence
6.1	Process documented for Data Principals to submit access requests and obtain: (a) summary of data processed, (b) identities of all DFs/DPs data shared with, (c) other prescribed info	☐	☐	☐	Sec 11(1)
6.2	Access requests responded to within 90 days as per DPDP Rules 2025 (NOT 30 days — that is a GDPR timeline)	☐	☐	☐	Rules 2025
6.3	Information provided in accessible, machine-readable format (PDF/CSV); no excessive fees charged	☐	☐	☐	Sec 11(1)
Section Score: _____ / ___ | Critical Gaps Noted: _____					

6B. RIGHT TO CORRECTION & ERASURE — SECTION 12					
#	Requirement	Yes	No	N/A	Section Ref / Evidence

6.4	Users can correct inaccurate/misleading personal data; incomplete data can be completed; outdated data can be updated	☐	☐	☐	Sec 12(1)-(2)
6.5	Third-party Data Fiduciaries / Processors notified of corrections where data was previously shared	☐	☐	☐	Sec 12(2)
6.6	Clear erasure (deletion) mechanism exists; deletion actually removes data from active systems, backups, archives (within retention law limits)	☐	☐	☐	Sec 12(3)
6.7	Exceptions to erasure clearly documented: data retained only where legally mandated (e.g., RBI/SEBI/Income Tax requirements)	☐	☐	☐	Sec 12(3)

Section Score: _____ / ___ | Critical Gaps Noted: _____

6C. RIGHT TO GRIEVANCE REDRESSAL — SECTION 13

#	Requirement	Yes	No	N/A	Section Ref / Evidence
6.8	Grievance redressal mechanism established and easily accessible to Data Principals [Sec 8(10) & 13(1)]	☐	☐	☐	Sec 8(10), 13(1)
6.9	Grievances responded to within 30 days as per DPDP Rules 2025 [Sec 13(2)]	☐	☐	☐	Sec 13(2)
6.10	Data Principal informed of escalation path to DPBI after exhausting grievance mechanism [Sec 13(3)]	☐	☐	☐	Sec 13(3)

Section Score: _____ / ___ | Critical Gaps Noted: _____

6D. RIGHT TO NOMINATE — SECTION 14 (UNIQUE TO DPDP)

#	Requirement	Yes	No	N/A	Section Ref / Evidence
6.11	Mechanism for Data Principal to nominate another individual to exercise data rights in event of death or incapacity established	☐	☐	☐	Sec 14(1)
6.12	Nomination records maintained securely; process for verifying and acting upon nomination in case of Data Principal's death/incapacity documented	☐	☐	☐	Sec 14(1)-(2)

Section Score: _____ / ___ | Critical Gaps Noted: _____

Section 7: Data Security Measures [13 Points]

Failure to maintain reasonable security safeguards is the HIGHEST PENALTY provision under DPDP Act — up to ₹250 Crore [Schedule Item 1, Sec 8(5)]

7A. TECHNICAL SECURITY — SECTION 8(4)-(5)

#	Requirement	Yes	No	N/A	Section Ref / Evidence
7.1	Personal data encrypted AT REST using industry-standard encryption (AES-256 or equivalent)	☐	☐	☐	Sec 8(5)
7.2	Personal data encrypted IN TRANSIT using TLS 1.2 or higher (HTTPS enforced on all endpoints)	☐	☐	☐	Sec 8(5)
7.3	Multi-Factor Authentication (MFA) enabled for all systems processing personal data	☐	☐	☐	Sec 8(4)-(5)
7.4	Role-Based Access Control (RBAC) implemented; Principle of Least Privilege enforced	☐	☐	☐	Sec 8(4)
7.5	Intrusion Detection / Prevention System (IDS/IPS) and real-time breach detection monitoring in place	☐	☐	☐	Sec 8(5), Rules 2025
7.6	Regular security patches applied; vulnerability assessments and penetration testing conducted at least annually	☐	☐	☐	Sec 8(4)-(5)
7.7	Access logs maintained; all access to personal data systems logged and auditable	☐	☐	☐	Rules 2025, Sec 8(5)
7.8	Session timeout / auto-logout configured on all systems storing or accessing personal data	☐	☐	☐	Sec 8(4)

Section Score: _____ / ___ | Critical Gaps Noted:
_____

7B. ORGANISATIONAL SECURITY — SECTION 8(4)

#	Requirement	Yes	No	N/A	Section Ref / Evidence
7.9	Information Security Policy documented, approved by senior management, and communicated to all staff	☐	☐	☐	Sec 8(4)
7.10	All employees with access to personal data trained on DPDP obligations and data handling procedures; training records maintained	☐	☐	☐	Sec 8(4)
7.11	Non-Disclosure Agreements (NDAs) incorporating data protection obligations signed by relevant employees and contractors	☐	☐	☐	Sec 8(2)
7.12	Secure data disposal procedures in place: digital data securely wiped (DoD standards); physical records shredded	☐	☐	☐	Sec 8(7)
7.13	Business Continuity and Disaster Recovery Plans documented, tested at minimum annually	☐	☐	☐	Sec 8(5)

Section Score: _____ / ___ | Critical Gaps Noted:
_____

Section 8: Children's Data [10 Points]

Mark entire section N/A only if the organisation's platform/service definitively does not and cannot collect data from individuals under 18.

8. CHILDREN'S DATA — SECTION 9, DPDP ACT 2023 (Penalty up to ₹200 Crore for violations)					
#	Requirement	Yes	No	N/A	Section Ref / Evidence
8.1	Age verification mechanism in place — technological means deployed to determine if user is under 18 years	☐	☐	☐	Sec 9(1), (5)
8.2	VERIFIABLE parental/guardian consent obtained before any personal data of users under 18 is processed	☐	☐	☐	Sec 9(1)
8.3	Process for verifying identity of consenting parent/guardian is documented and operational	☐	☐	☐	Sec 9(1)
8.4	ZERO targeted advertising directed at children — no ad-targeting algorithms applied to users under 18	☐	☐	☐	Sec 9(3)
8.5	ZERO behavioural monitoring or tracking of children — no profiling, no tracking cookies, no behavioural analytics for users under 18	☐	☐	☐	Sec 9(3)
8.6	No processing of children's data likely to cause detrimental effect on child's well-being [Sec 9(2)]	☐	☐	☐	Sec 9(2)
8.7	Where Rules 2025 exceptions apply (healthcare, education, real-time safety), processing is strictly limited to that exempted purpose	☐	☐	☐	Sec 9(4), Rules 2025
8.8	Parents/guardians can access, correct, and request deletion of their child's personal data	☐	☐	☐	Sec 9, 12
8.9	Age-appropriate, simplified privacy notices prepared for child users (plain language, visually accessible)	☐	☐	☐	Rules 2025, Sec 5(3)
8.10	Enhanced security measures applied to systems storing children's personal data	☐	☐	☐	Sec 8(5), 9
Section Score: _____ / ___ | Critical Gaps Noted: _____					

Section 9: Cross-Border Data Transfers [5 Points]

DPDP Act adopts a BLACKLIST approach (Sec 16(1)) — transfers permitted to all countries EXCEPT those specifically notified/restricted by Central Government. This is different from GDPR (whitelist/adequacy). 'Standard Contractual Clauses' are a GDPR concept and do not apply under DPDP.

9. CROSS-BORDER DATA TRANSFERS — SECTION 16, DPDP ACT 2023

#	Requirement	Yes	No	N/A	Section Ref / Evidence
9.1	All cross-border personal data transfers mapped and documented (country, purpose, data category, transferee entity)	☐	☐	☐	Sec 16(1)
9.2	Transfers monitored against Central Government blacklist notifications under Sec 16(1) — no data transferred to notified/restricted countries	☐	☐	☐	Sec 16(1)
9.3	Sectoral data localisation requirements met: payment data (RBI mandate), health data (sector specific), financial data — respective regulator mandates reviewed	☐	☐	☐	Sec 16(2)
9.4	Contract with overseas Data Processor contains DPDP obligations equivalent provisions (valid contract requirement under Sec 8(2))	☐	☐	☐	Sec 8(2)
9.5	Process established to monitor Central Government blacklist updates and respond within compliance timelines	☐	☐	☐	Sec 16(1), Rules 2025

Section Score: _____ / ___ | Critical Gaps Noted: _____

Section 10: Personal Data Breach Preparedness [10 Points]

Failure to maintain security safeguards → ₹250 Cr penalty [Schedule Item 1]. Failure to notify DPBI/affected individuals → ₹200 Cr penalty [Schedule Item 2, Sec 8(6)].

10. PERSONAL DATA BREACH PREPAREDNESS — SECTION 8(6), DPDP RULES 2025

#	Requirement	Yes	No	N/A	Section Ref / Evidence
10.1	Incident Response Plan (IRP) for personal data breaches documented — defines roles, escalation path, decision tree	☐	☐	☐	Sec 8(6)
10.2	Incident Response Team (IRT) constituted — includes legal, technical, communications, and senior management representatives	☐	☐	☐	Sec 8(6)
10.3	Real-time breach detection monitoring operational: SIEM, logging systems, alert thresholds configured	☐	☐	☐	Rules 2025
10.4	IMMEDIATE notification to ALL affected Data Principals without delay upon discovery of breach — plain language message explaining: what happened, possible impact, steps taken, contact details [Rules 2025]	☐	☐	☐	Sec 8(6), Rules 2025
10.5	DPBI breach notification process defined; contact information for Data Protection Board documented and accessible to IRT	☐	☐	☐	Sec 8(6), Rules 2025

10.6	Detailed breach report submitted to DPBI within 72 hours of initial intimation [DPDP Rules 2025]	☐	☐	☐	Rules 2025
10.7	Breach severity assessment process documented: determines reportability threshold, impact scope, data categories involved	☐	☐	☐	Sec 33(2)
10.8	Pre-drafted breach notification templates available (for individuals and DPBI)	☐	☐	☐	Rules 2025
10.9	IRP tested / tabletop exercise simulated at least annually; test results documented	☐	☐	☐	Sec 10(2)(c)(ii) for SDF
10.10	Breach log maintained: all incidents (including minor ones) documented with date, nature, scope, actions taken, notification status	☐	☐	☐	Sec 28(7)(c)
Section Score: _____ / ___ | Critical Gaps Noted: _____					

Section 11: Vendor & Third-Party Management (Data Processors) [10 Points]

Under Sec 8(1), the Data Fiduciary remains liable for breaches by Data Processors. The Data Processor is bound by a valid contract only — primary legal responsibility sits with the Data Fiduciary.

11. VENDOR & DATA PROCESSOR MANAGEMENT — SECTIONS 8(1)-(2), DPDP ACT 2023

#	Requirement	Yes	No	N/A	Section Ref / Evidence
11.1	Complete inventory of all vendors / third parties with access to personal data maintained	☐	☐	☐	Sec 8(1)-(2)
11.2	Data Processing Agreements (DPAs) — VALID CONTRACTS — executed with ALL Data Processors before any processing begins [Sec 8(2)]	☐	☐	☐	Sec 8(2)
11.3	DPAs contain: DPDP compliance obligations, security requirements, breach notification duties, data deletion on contract termination	☐	☐	☐	Sec 8(2)
11.4	DPAs include: prohibition on sub-contracting without written consent; equivalent obligations flow down to sub-processors	☐	☐	☐	Sec 8(1)-(2)
11.5	Vendor security assessments conducted before onboarding — includes review of their data protection practices	☐	☐	☐	Sec 8(4)-(5)
11.6	Regular vendor compliance reviews / audits conducted (minimum annually for high-risk vendors)	☐	☐	☐	Sec 8(1)
11.7	Vendor access to personal data monitored, logged, and access revoked immediately upon contract termination	☐	☐	☐	Sec 8(4)-(5)
11.8	Vendor offboarding process ensures personal data deletion / return is verified and documented	☐	☐	☐	Sec 8(7)
11.9	Data Processor engaged only for activities 'related to offering of goods or services to Data Principals' as required by Sec 8(2)	☐	☐	☐	Sec 8(2)
11.10	Organisation as Data Processor (if applicable): operates only within scope of valid contract with Data Fiduciary; no independent use of Data Principal data	☐	☐	☐	Sec 2(k)

Section Score: _____ / ___ | Critical Gaps Noted: _____

Section 12: Documentation & Governance [10 Points]

12A. REQUIRED DOCUMENTS

#	Requirement	Yes	No	N/A	Section Ref / Evidence
12.1	Privacy Notice/Policy published and prominently accessible on all platforms (website, app, physical premises)	☐	☐	☐	Sec 5, 8(9)

12.2	Privacy Notice covers all DPDP-required elements: data collected, purpose, rights, grievance mechanism, DPO/contact details	☐	☐	☐	Sec 5(1), 8(9)
12.3	Privacy Notice available in English AND at least one 8th Schedule language [Sec 5(3)]; translations are accurate	☐	☐	☐	Sec 5(3)
12.4	Data Retention Policy documented and operationalised — specifies retention periods per data category and auto-deletion triggers	☐	☐	☐	Sec 8(7)-(8)
12.5	Consent management records maintained (see Section 4B above)	☐	☐	☐	Sec 6(10)
12.6	Employee data protection training materials and attendance records maintained	☐	☐	☐	Sec 8(4)

Section Score: _____ / ___ | Critical Gaps Noted: _____

12B. GOVERNANCE STRUCTURE

#	Requirement	Yes	No	N/A	Section Ref / Evidence
12.7	Clear accountability for DPDP compliance assigned at senior level (CISO / DPO / Legal Counsel)	☐	☐	☐	Sec 8(1)
12.8	Data protection responsibilities explicitly included in relevant job descriptions / KRAs	☐	☐	☐	Sec 8(4)
12.9	Board / Senior Management oversight of data protection compliance established; compliance reported quarterly at minimum	☐	☐	☐	Sec 10(2)(a) for SDF
12.10	Budget allocated for DPDP compliance implementation and ongoing maintenance	☐	☐	☐	Sec 8(4)

Section Score: _____ / ___ | Critical Gaps Noted: _____

12C. PRIVACY BY DESIGN

#	Requirement	Yes	No	N/A	Section Ref / Evidence
12.11	Privacy considered in all new product/feature development before launch — privacy review as part of product approval process	☐	☐	☐	Sec 8(4), Rules 2025
12.12	Default settings are privacy-protective — most restrictive data sharing settings applied by default	☐	☐	☐	Rules 2025
12.13	Regular privacy compliance audits scheduled; continuous improvement process for data protection in place	☐	☐	☐	Sec 10(2)(c)(ii)

Section Score: _____ / ___ | Critical Gaps Noted: _____

Special Section: Significant Data Fiduciary (SDF) Assessment

APPLICABILITY: Complete this section ONLY if the organisation has been notified as a Significant Data Fiduciary (SDF) by the Central Government under Section 10(1) of the DPDP Act.

SDF Notification Factors [Sec 10(1)]: (a) Volume & sensitivity of data processed, (b) Risk to Data Principals' rights, (c) Impact on sovereignty & integrity of India, (d) Risk to electoral democracy, (e) Security of the State, (f) Public order. Likely SDFs: Major social media platforms, large fintech entities, health data aggregators, entities processing electoral data.

SDF. ADDITIONAL OBLIGATIONS OF SIGNIFICANT DATA FIDUCIARY — SECTION 10(2)

#	Requirement	Yes	No	N/A	Section Ref / Evidence
S.1	DATA PROTECTION OFFICER (DPO) appointed — individual (not a firm), based in India, responsible to Board of Directors [Sec 10(2)(a)]	☐	☐	☐	Sec 10(2)(a)
S.2	DPO is the designated point of contact for grievance redressal mechanism under DPDP Act [Sec 10(2)(a)(iv)]	☐	☐	☐	Sec 10(2)(a)(iv)
S.3	DPO contact details published on website/app as per Sec 8(9); easily accessible to Data Principals	☐	☐	☐	Sec 8(9)
S.4	INDEPENDENT DATA AUDITOR appointed — external, independent (not in-house); evaluates SDF's DPDP compliance [Sec 10(2)(b)]	☐	☐	☐	Sec 10(2)(b)
S.5	PERIODIC DATA PROTECTION IMPACT ASSESSMENT (DPIA) conducted — includes: description of Data Principals' rights, purpose of processing, risk assessment & management [Sec 10(2)(c)(i)]	☐	☐	☐	Sec 10(2)(c)(i)
S.6	PERIODIC AUDIT conducted (internal and/or external) [Sec 10(2)(c)(ii)]	☐	☐	☐	Sec 10(2)(c)(ii)
S.7	Additional prescribed measures complied with as may be notified by Central Government [Sec 10(2)(c)(iii)]	☐	☐	☐	Sec 10(2)(c)(iii)
S.8	Restricted data categories and localisation requirements (per Rules 2025 / sector regulator directions) met	☐	☐	☐	Rules 2025
S.9	Process to comply with Central Government blocking directions under Sec 37 in place; appeal mechanism documented	☐	☐	☐	Sec 37
S.10	Voluntary Undertaking procedure documented — board-level authority identified to accept/issue undertakings under Sec 32	☐	☐	☐	Sec 32

Section Score: _____ / ___ | Critical Gaps Noted: _____

Overall Compliance Summary

Section	Max	Score	%	Key Gaps
1. Data Inventory & Mapping	10	___	___ %	_____
2. Legal Basis for Processing	10	___	___ %	_____
3. Notice Requirements (DPDP-Specific)	10	___	___ %	_____
4. Consent Management	15	___	___ %	_____
5. Legitimate Uses Assessment	5	___	___ %	_____
6. Individual Rights (Data Principal Rights)	12	___	___ %	_____
7. Data Security Measures	13	___	___ %	_____
8. Children's Data (if applicable)	10	___	___ %	_____
9. Cross-Border Data Transfers	5	___	___ %	_____
10. Personal Data Breach Preparedness	10	___	___ %	_____
11. Vendor & Third-Party Management	10	___	___ %	_____
12. Documentation & Governance	10	___	___ %	_____
TOTAL	**100**	___	___ %	_____

Compliance Rating Scale

Score	Rating & Interpretation	Recommended Action
90 – 100	EXCELLENT COMPLIANCE — Minimal gaps; strong governance; Board-audit ready	Schedule annual re-audit; monitor Rule updates
75 – 89	GOOD COMPLIANCE — Solid foundation; minor gaps to address within 90 days	Prioritise Sections scoring < 7/10; 60-day plan
60 – 74	FAIR COMPLIANCE — Moderate gaps; structured remediation plan required	Immediate action on red-flag items; 90-day plan
45 – 59	POOR COMPLIANCE — Significant gaps; substantial work needed immediately	Engage DPO/legal counsel; 30-day crisis plan
< 45	NON-COMPLIANT — Critical gaps; high risk of Board penalties up to ₹250 Cr	Stop high-risk processing; legal advice immediately

Critical Red Flags — Immediate Action Required

The following items, if marked 'No' during audit, constitute HIGH-RISK compliance failures requiring action within 30 days. All carry potential penalties between ₹50 Crore and ₹250 Crore under the DPDP Act Schedule.

Critical Red Flag	Act / Penalty Reference	Immediate Action Required
No valid consent mechanism whatsoever	Sec 6 | Rules 2025	Immediately stop processing or face ₹250 Cr penalty
No notice provided before collecting personal data	Sec 5	Notices must precede every consent request
Children's data processed without verifiable parental consent	Sec 9(1) | ₹200 Cr penalty	Suspend processing; implement age verification
No encryption of personal data (at rest or in transit)	Sec 8(5) | ₹250 Cr penalty	Implement AES-256 & TLS 1.2+ immediately
No personal data breach response plan	Sec 8(6)	Draft and test IRP; set up DPBI contact
Personal data shared with vendors without a valid contract	Sec 8(2)	Execute DPAs with all data processors immediately
No mechanism for users to delete / erase their data	Sec 12(3)	Build erasure workflow within 30 days
No privacy notice / policy published	Sec 5 & 8(9)	Draft and publish on all platforms
Data retained indefinitely with no retention policy	Sec 8(7)	Define retention periods; implement auto-deletion
Notice not available in any Indian language (8th Schedule)	Sec 5(3) & 6(3)	Localise notices into required languages
Employees have unrestricted access to all personal data	Sec 8(4)	Implement RBAC / least-privilege immediately
SDF has not appointed a DPO based in India	Sec 10(2)(a)	Appoint DPO; register with Board
No grievance redressal mechanism established	Sec 8(10) & 13	Set up grievance portal within 30 days
No response to Data Principal rights requests within 90 days	Sec Rules 2025	Build rights-management workflow

Critical Findings (Reviewer Narrative)

#	Priority	Finding	Section Reference
1			
2			
3			
4			
5			
6			

#	Priority	Finding	Section Reference
7			
8			

Priority Action Plan

IMMEDIATE (Month 1) — Critical Red Flags

Action Item	Responsible Party	Deadline	Budget	Status

SHORT-TERM (Months 2–3) — High Priority Gaps

Action Item	Responsible Party	Deadline	Budget	Status

MEDIUM-TERM (Months 4–9) — Compliance Build-Out

Action Item	Responsible Party	Deadline	Budget	Status

LONG-TERM (Months 10–18) — Full Operationalisation

Action Item	Responsible Party	Deadline	Budget	Status

Estimated Compliance Investment Required

Compliance Category	Estimated Cost (₹)	Priority	Timeline
Legal / Policy Documentation (Privacy Notice, DPAs, Consent frameworks)	₹ _____	**HIGH**	Month 1-2
Technical Implementation (Encryption, MFA, RBAC, Access Logs)	₹ _____	**HIGH**	Month 1-3
Consent Management System / Platform	₹ _____	**HIGH**	Month 1-3
Grievance & Rights Request Management Portal	₹ _____	**HIGH**	Month 2-4
Breach Response Infrastructure (SIEM, IRP tools)	₹ _____	**HIGH**	Month 1-3
Employee Training & Awareness Programme	₹ _____	MEDIUM	Month 2-4
DPO Services (if outsourced — SDF only)	₹ _____	**HIGH (SDF)**	Month 1
Independent Data Audit (SDF only)	₹ _____	**HIGH (SDF)**	Annually
DPIA Exercise (SDF only)	₹ _____	**HIGH (SDF)**	Bi-annually
Vendor DPA Execution & Vendor Risk Assessments	₹ _____	**HIGH**	Month 1-3
Multilingual Notice Localisation (22 languages)	₹ _____	MEDIUM	Month 3-6
Ongoing Compliance Monitoring & Annual Re-audit	₹ _____	MEDIUM	Annual
TOTAL ESTIMATED INVESTMENT	₹ _____		18 months

Next Steps & Reviewer Recommendations

1. Review audit findings with senior management and legal counsel within 7 days of receiving this report
2. Approve action plan and allocate remediation budget — obtain Board/management sign-off
3. Assign named responsible parties for each action item in the Priority Action Plan
4. Engage a qualified Data Protection Officer (DPO) or legal counsel for ongoing DPDP compliance advisory
5. Begin implementation of all Immediate (Month 1) priority items without delay
6. Monitor Central Government notifications for SDF lists and country blacklists under Sec 16(1) regularly
7. Schedule follow-up re-audit within 6 months to track remediation progress
8. Subscribe to DPBI and MEITY notifications for updates to Rules, guidelines and enforcement actions

Reviewer & Client Sign-Off

REVIEWER (AUDITOR)	
Reviewed by (Name): _____	Bar Enrolment No.: _____
Designation / Firm: _____	Date of Report: _____
Signature: _____	: _____
CLIENT ACKNOWLEDGEMENT	
Acknowledged by (Name): _____	Designation / Title: _____
Organisation: _____	Date: _____
Signature: _____	: _____

Appendices

- Appendix A: Data Flow Maps
- Appendix B: Complete Vendor / Data Processor Inventory
- Appendix C: Sample Privacy Notice Template (DPDP Act 2023 compliant)
- Appendix D: Sample Consent Mechanism Screenshots / Records
- Appendix E: Data Processing Agreement (DPA) Template
- Appendix F: Breach Notification Template (for DPBI and Data Principals)
- Appendix G: Supporting Evidence — Policies, Screenshots, System Records
- Appendix H: Summary of Central Government Notifications (SDF lists, blacklists) as of audit date

— End of DPDP Act 2023 & Rules 2025 Compliance Audit Report —

Prepared in accordance with the Digital Personal Data Protection Act, 2023 (No. 22 of 2023) and Digital Personal Data Protection Rules, 2025