securion.ai

DPDP ACT 2023 · DPDP RULES 2025

DPDPA Readiness Checklist

53 controls across 7 domains. Score each control **Not started / Partial / Implemented**, name an owner, and keep the evidence current for the day the Data Protection Board asks.

How to use: Domains A–D and F–G are the privacy-governance obligations that ISO 27001 does **not** cover. Domain E (Rule 6 security safeguards) maps directly onto your ISO 27001 / SOC 2 controls — if you already run those, start there.

#	REQUIREMENT	ACT / RULE	STATUS	OWNER / EVIDENCE
A	**Governance & Accountability**			
A.1	Assign accountability for data protection (grievance/contact officer; DPO if a Significant Data Fiduciary)	S.8(9)–(10), S.10	☐ Not started ☐ Partial ☐ Implemented	
A.2	Publish and operate a grievance-redressal mechanism with defined response timelines	S.8(10), S.13	☐ Not started ☐ Partial ☐ Implemented	
A.3	(SDF) Appoint an independent Data Auditor and undergo periodic data audits	S.10, DPDP Rules 2025 (SDF)	☐ Not started ☐ Partial ☐ Implemented	
A.4	(SDF) Conduct periodic Data Protection Impact Assessments (DPIAs)	S.10, DPDP Rules 2025 (SDF)	☐ Not started ☐ Partial ☐ Implemented	
A.5	Maintain a documented data-protection / privacy policy (internal and published)	S.8 (accountability)	☐ Not started ☐ Partial ☐ Implemented	
A.6	Run staff training and awareness on DPDPA obligations	S.8 (accountability)	☐ Not started ☐ Partial ☐ Implemented	
A.7	Keep accountability records (roles, decisions, evidence of compliance)	S.8	☐ Not started ☐ Partial ☐ Implemented	
A.8	(SDF) Implement any additional measures the government prescribes (e.g. due-diligence of processing)	S.10, DPDP Rules 2025 (SDF)	☐ Not started ☐ Partial ☐ Implemented	
B	**Lawful Basis, Notice & Consent**			

#	REQUIREMENT	ACT / RULE	STATUS	OWNER / EVIDENCE
B.1	Establish a valid legal basis (consent or a listed legitimate use) for every processing activity	S.4, S.7	☐ Not started ☐ Partial ☐ Implemented	
B.2	Provide a clear, itemised notice before/at the point of consent (data, purpose, rights, how to complain)	S.5, DPDP Rules 2025 (notice)	☐ Not started ☐ Partial ☐ Implemented	
B.3	Make notice available in English and the 22 Eighth-Schedule languages	S.5(3)	☐ Not started ☐ Partial ☐ Implemented	
B.4	Obtain consent that is free, specific, informed, unconditional and unambiguous	S.6(1)	☐ Not started ☐ Partial ☐ Implemented	
B.5	Provide withdrawal of consent that is as easy as giving it	S.6(4)–(6)	☐ Not started ☐ Partial ☐ Implemented	
B.6	Maintain consent records/logs (versioned, timestamped, purpose-linked)	S.6, DPDP Rules 2025	☐ Not started ☐ Partial ☐ Implemented	
B.7	Integrate with a registered Consent Manager where applicable	S.6(7)–(9), DPDP Rules 2025	☐ Not started ☐ Partial ☐ Implemented	
B.8	Do not bundle or condition consent on unrelated services	S.6(1)	☐ Not started ☐ Partial ☐ Implemented	
B.9	Provide retrospective notice for personal data collected before the Act	S.5(2)	☐ Not started ☐ Partial ☐ Implemented	
B.10	Obtain verifiable parental consent + age assurance for children (<18); no tracking or targeted ads	S.9, DPDP Rules 2025 (children)	☐ Not started ☐ Partial ☐ Implemented	
C	**Data Principal Rights**			
C.1	Operate a Right to Access (summary of data processed and recipients)	S.11	☐ Not started ☐ Partial ☐ Implemented	

#	REQUIREMENT	ACT / RULE	STATUS	OWNER / EVIDENCE
C.2	Operate Rights to Correction, Completion, Updating and Erasure	S.12	☐ Not started ☐ Partial ☐ Implemented	
C.3	Operate a Right to Grievance Redressal (before approaching the Board)	S.13	☐ Not started ☐ Partial ☐ Implemented	
C.4	Support the Right to Nominate another person to exercise rights	S.14	☐ Not started ☐ Partial ☐ Implemented	
C.5	Publish the contact/means for Data Principals to exercise their rights	S.5, DPDP Rules 2025	☐ Not started ☐ Partial ☐ Implemented	
C.6	Define and publish response timelines for rights requests	S.13, DPDP Rules 2025	☐ Not started ☐ Partial ☐ Implemented	
C.7	Verify the identity of a requester before actioning a rights request	S.11–12 (implementation)	☐ Not started ☐ Partial ☐ Implemented	
D	**Data Lifecycle & Governance**			
D.1	Enforce purpose limitation — process only for the stated purpose	S.6, S.8(1)	☐ Not started ☐ Partial ☐ Implemented	
D.2	Apply data minimisation — collect only what is necessary	S.6(1)	☐ Not started ☐ Partial ☐ Implemented	
D.3	Keep personal data accurate where used to make decisions or shared	S.8(3)–(4)	☐ Not started ☐ Partial ☐ Implemented	
D.4	Enforce retention limits — erase when purpose is served or consent withdrawn (unless law requires)	S.8(7), DPDP Rules 2025 (retention)	☐ Not started ☐ Partial ☐ Implemented	
D.5	Maintain a Record of Processing / data inventory (personal data, purposes, flows, processors)	S.8 (accountability)	☐ Not started ☐ Partial ☐ Implemented	

#	REQUIREMENT	ACT / RULE	STATUS	OWNER / EVIDENCE
D.6	Classify personal data and identify sensitive categories and children's data	S.8–9 (implementation)	☐ Not started ☐ Partial ☐ Implemented	
D.7	Map data flows across processors and geographies	S.8, S.16 (implementation)	☐ Not started ☐ Partial ☐ Implemented	
D.8	Automate / schedule deletion to enforce retention limits	S.8(7), DPDP Rules 2025	☐ Not started ☐ Partial ☐ Implemented	
E	**Security Safeguards — Rule 6 (maps to ISO 27001)**			
E.1	Encrypt / mask / obfuscate / tokenise personal data (at rest and in transit)	Rule 6	☐ Not started ☐ Partial ☐ Implemented	
E.2	Enforce access controls to systems processing personal data (least privilege, MFA)	Rule 6	☐ Not started ☐ Partial ☐ Implemented	
E.3	Log, monitor and review access to personal data (detect, investigate, remediate)	Rule 6	☐ Not started ☐ Partial ☐ Implemented	
E.4	Retain access logs for at least one year	Rule 6	☐ Not started ☐ Partial ☐ Implemented	
E.5	Maintain backups and resilience for continued processing after compromise	Rule 6	☐ Not started ☐ Partial ☐ Implemented	
E.6	Implement breach-detection measures	Rule 6, Rule 7	☐ Not started ☐ Partial ☐ Implemented	
E.7	Bind Data Processors by contract to the same reasonable security safeguards	S.8(2), Rule 6	☐ Not started ☐ Partial ☐ Implemented	
E.8	Maintain confidentiality, integrity and availability of personal data (general safeguards)	Rule 6	☐ Not started ☐ Partial ☐ Implemented	

#	REQUIREMENT	ACT / RULE	STATUS	OWNER / EVIDENCE
E.9	Run secure configuration, patching and vulnerability management	Rule 6 (reasonable safeguards)	☐ Not started ☐ Partial ☐ Implemented	
F	**Breach Management — Rule 7**			
F.1	Detect and triage personal data breaches	Rule 6, Rule 7	☐ Not started ☐ Partial ☐ Implemented	
F.2	Notify affected Data Principals without delay, in clear language	Rule 7	☐ Not started ☐ Partial ☐ Implemented	
F.3	Report a detailed breach account to the Data Protection Board within 72 hours	Rule 7	☐ Not started ☐ Partial ☐ Implemented	
F.4	Include the required content in breach notices (nature, consequences, mitigation, safety steps, contact)	Rule 7	☐ Not started ☐ Partial ☐ Implemented	
F.5	Maintain a breach register	Rule 7	☐ Not started ☐ Partial ☐ Implemented	
F.6	Carry out post-incident remediation to prevent recurrence	Rule 6–7	☐ Not started ☐ Partial ☐ Implemented	
G	**Third Parties & Cross-Border**			
G.1	Put Data Processing Agreements in place binding vendors to DPDPA safeguards	S.8(2)	☐ Not started ☐ Partial ☐ Implemented	
G.2	Conduct vendor due diligence / periodic security reviews	S.8(2), Rule 6	☐ Not started ☐ Partial ☐ Implemented	
G.3	Flow down obligations to sub-processors	S.8(2)	☐ Not started ☐ Partial ☐ Implemented	
G.4	Maintain a cross-border transfer register	S.16	☐ Not started ☐ Partial ☐ Implemented	

#	REQUIREMENT	ACT / RULE	STATUS	OWNER / EVIDENCE
G.5	Screen transfers against government-restricted countries	S.16	☐ Not started ☐ Partial ☐ Implemented	

Prepared by Securion.ai. Covers the security and evidence side of DPDPA readiness; not a substitute for legal advice on consent, notice, and lawful basis. Securion maps your systems to these controls and monitors them continuously — securion.ai.