DIGITAL PERSONAL DATA PROTECTION

Compliance Audit & Gap Analysis Report

Statutory Readiness Review under the Digital Personal Data Protection Act, 2023 (DPDP Act), IT (SPDI) Rules 2011, and CERT-In Cyber Security Directions.

Prepared by Prem Singh, WebCompliance.in

Generated with Compliance Audit WC Software

■■ **DRAFT CONTENT AUDIT — NOT VERIFIED FOR FORMAL CLIENT RELIANCE**

This report was generated using draft regulatory rules and pilot rule sets. Statutory interpretations and rule citations remain subject to official gazette notification.

Audited Organisation:	Acme Cloud Solutions Pvt Ltd
Legal Entity Name:	Acme Cloud Solutions Private Limited
Industry / Segment:	IT / SaaS
Prepared by:	Prem Singh, WebCompliance.in
Active Content Pack:	india_data_protection_v1_draft (v0.1.0)
Audit Assessment Date:	2026-10-26
Lead Compliance Auditor:	Prem Singh
Audit Status:	COMPLETED & COMMITTED
Cryptographic Verification:	aa0d17d71d9811b1e1f30f7b35e4638b...

CONFIDENTIALITY NOTICE: The information contained in this document is strictly confidential. It is intended exclusively for the management of the audited entity. Any unauthorized distribution, copying, or disclosure is strictly prohibited.

CONFIDENTIAL DRAFT — NOT VERIFIED

1. Executive Summary

This report summarizes the comprehensive statutory privacy audit conducted on-site. Evaluations covered thirty-one core statutory controls spanning governance, consent management, data principal rights, security safeguards, cross-border transfers, and breach response protocols.

33.3%	6	42	48
Overall Readiness	**Current Exposure**	**DPDP Readiness**	**Total Action Items**
31 statutory controls	~~0 Critical, 6 High~~	~~11 Critical, 10 High~~	Prioritized roadmap

Regulatory Timeline & Enforcement Milestones:

Milestone	Date	Timeline Status
IT Act s.72A in force	2009-10-27	In force (6208 days prior to audit)
SPDI Rules 2011 commencement	2011-04-11	In force (5677 days prior to audit)
CERT-In Directions of 28 April 2022 effective	2022-06-27	In force (1582 days prior to audit)
DPDP phase 1 - publication of commencement notification and Rules	2025-11-13	In force (347 days prior to audit)
DPDP phase 2 - one year after publication (Consent Managers)	2026-11-13	18 days from audit date
DPDP phase 3 - eighteen months after publication (substantive obligations)	2027-05-13	199 days from audit date

Top 5 current risks (in force today):

Rule & Citation	Control	Penalty Band	Risk Score	Priority
CERTIN-DIR-III-ORDER-COMPLIANCE: Act on, or provide information demanded by, a CERT-In order within its timeframe CERT-In Directions 28.04.2022, Direction (iii) (first part)	**CTL-GOV-03** Disclosure authorisation and authority-request handling	**HIGH**	**290.0**	**High**
ITACT-S72A-CONTRACT-DISCLOSURE: Do not disclose personal information obtained under a service contract without consent or in breach of contract IT Act 2000 s.72A	**CTL-GOV-03** Disclosure authorisation and authority-request handling	**HIGH**	**290.0**	**High**
SPDI-R6-1-DISCLOSURE-PERMISSION: Obtain prior permission before disclosing SPDI to a third party SPDI Rules 2011 r.6(1)	**CTL-GOV-03** Disclosure authorisation and authority-request handling	**HIGH**	**290.0**	**High**
SPDI-R6-3-NO-PUBLICATION: Do not publish SPDI SPDI Rules 2011 r.6(3)	**CTL-GOV-03** Disclosure authorisation and authority-request handling	**HIGH**	**290.0**	**High**
SPDI-R6-4-NO-ONWARD-DISCLOSURE: A third party receiving SPDI must not disclose it further SPDI Rules 2011 r.6(4)	**CTL-GOV-03** Disclosure authorisation and authority-request handling	**HIGH**	**290.0**	**High**

CONFIDENTIAL DRAFT - NOT VERIFIED

2. Audit Scope & Regulatory Framework

Statutory Basis: This compliance assessment was conducted in accordance with the regulatory framework established under the **india_data_protection_v1_draft** content pack (v0.1.0), evaluating organizational controls against the following statutory authorities:

- **CERT-In Directions:** 7 statutory rules evaluated.
- **Digital Personal Data Protection (DPDP):** 42 statutory rules evaluated.
- **Information Technology Act (IT Act):** 1 statutory rules evaluated.
- **IT (SPDI) Rules:** 14 statutory rules evaluated.

CONFIDENTIAL
DRAFT — NOT VERIFIED

Organisational Profile & Scope Inputs:

Scope Question / Parameter	Recorded Fact / Status
What is the legal form of your organisation?	**Private or public limited company**
Roughly how many people work for you, including long-term contractors?	**45**
Is your organisation incorporated or registered in India?	**Yes**
Is any work involving information about people done in India - for example staff in India who can see it, or servers or cloud regions located in India?	**Yes**
Do you offer your product or services to individuals in India, including individual users who log in at your Indian client companies?	**Yes**
Do you hold or use any information in digital form about identifiable people - such as names, emails, phone numbers, IDs, user accounts, employee records or CVs?	**Yes**
For any of your activities, does your organisation itself decide why and how information about people is used?	**Yes**
Do you handle information about people on behalf of clients, where the client decides what it is used for?	**Yes**
Do you hold information about any individual who is located in India - including your own employees, job applicants, users or customer contacts?	**Yes**
Do you use information about people to make decisions that affect them - such as hiring, approving or suspending accounts, eligibility or pricing?	**Yes**
Do you share information about people with other organisations that use it for their own purposes (not just vendors working for you)?	**No**
Do you ask people to agree to how you use their information - for example a tick box, an "I agree" button or a signed form?	**Yes**
Do people send you their information for a specific purpose without a separate agree step - for example a contact form, an emailed CV or a demo request?	**Yes**
Do you still hold or use information about people who agreed to your use of it at some point in the past?	**Yes**
Do you use outside vendors or tools that store or work on information about people for you?	**Yes**
Is any information about people stored in, or accessed from, a country other than India?	**Yes**
While providing services under a contract, do you or your staff get access to information about people?	**Yes**
Do you hold or use information about anyone under 18?	**No**
Do you hold or use information about any adult with a disability who has a legally appointed guardian?	**No**
Do you store or handle any of the following about people - passwords, bank account or card details, health or medical information, sexual orientation, or biometrics (fingerprints, face data)?	**Yes**
Do you collect any of those items directly from the people concerned - for example when they set a password, enter card details or fill in a health form?	**Yes**
Which best describes what you provide to customers over the internet?	**Only our own software application, hosted by us, that customers log into**
What does your written advice from a qualified adviser conclude on whether your service counts as a "cloud service provider" under the CERT-In Directions of 28 April 2022?	**Written advice says we are not a cloud service provider for this purpose**
Do you operate a data centre, or rent out virtual private servers or server hosting to customers?	**No**

CONFIDENTIAL DRAFT — NOT VERIFIED

3. Findings Summary & Gap Register

The following register details all identified compliance gaps, mapped by control and affected statutory rule. Gaps are partitioned into current legal exposure and upcoming statutory readiness.

Part A: Current Legal Exposure

Statutory rules currently in force where mapped organizational controls require remediation:

Control	Statutory Rule & Title	Penalty Band	Score	Priority
CTL-GOV-03 Disclosure authorisation and authority-request handling	**CERTIN-DIR-III-ORDER-COMPLIANCE** (CERT-In Directions 28.04.2022, Direction (iii) (first part)) Act on, or provide information demanded by, a CERT-In order within its timeframe	**HIGH**	**290.0**	**High**
CTL-GOV-03 Disclosure authorisation and authority-request handling	**ITACT-S72A-CONTRACT-DISCLOSURE** (IT Act 2000 s.72A) Do not disclose personal information obtained under a service contract without consent or in breach of contract	**HIGH**	**290.0**	**High**
CTL-GOV-03 Disclosure authorisation and authority-request handling	**SPDI-R6-1-DISCLOSURE-PERMISSION** (SPDI Rules 2011 r.6(1)) Obtain prior permission before disclosing SPDI to a third party	**HIGH**	**290.0**	**High**
CTL-GOV-03 Disclosure authorisation and authority-request handling	**SPDI-R6-3-NO-PUBLICATION** (SPDI Rules 2011 r.6(3)) Do not publish SPDI	**HIGH**	**290.0**	**High**
CTL-GOV-03 Disclosure authorisation and authority-request handling	**SPDI-R6-4-NO-ONWARD-DISCLOSURE** (SPDI Rules 2011 r.6(4)) A third party receiving SPDI must not disclose it further	**HIGH**	**290.0**	**High**
CTL-GOV-02 Privacy compliance programme with accountable owner and staff training	**ITACT-S72A-CONTRACT-DISCLOSURE** (IT Act 2000 s.72A) Do not disclose personal information obtained under a service contract without consent or in breach of contract	**HIGH**	**181.2**	**High**

Part B: DPDP Readiness

Upcoming statutory rules whose mapped controls are not yet fully implemented or assessed, prioritized by commencement date:

Control	Upcoming Rule & Citation	Commences	Days Left	Penalty Band	Score	Priority
CTL-GOV-02 Privacy compliance programme with accountable owner and staff training	**DPDP-S8-5-SAFEGUARDS** (DPDP Act 2023 s.8(5); DPDP Rules 2025 r.6(1)(g)) Take reasonable security safeguards to prevent personal data breach	**2027-05-13**	199	**CRITICAL**	**362.5**	**Critical**
CTL-BRM-01 Personal data breach intimation procedure (Data Protection Board and affected individuals)	**DPDP-S8-6-DP-INTIMATION** (DPDP Act 2023 s.8(6); DPDP Rules 2025 r.7(1)(a)-(e)) Intimate each affected Data Principal of a personal data breach without delay	**2027-05-13**	199	**CRITICAL**	**290.0**	**High**
CTL-BRM-01 Personal data breach intimation procedure (Data Protection Board and affected individuals)	**DPDP-S8-6-BOARD-INITIAL** (DPDP Act 2023 s.8(6); DPDP Rules 2025 r.7(2)(a)) Initial intimation of a personal data breach to the Data Protection Board without delay	**2027-05-13**	199	**CRITICAL**	**290.0**	**High**

CONFIDENTIAL DRAFT — NOT VERIFIED

CTL-BRM-01 Personal data breach intimation procedure (Data Protection Board and affected individuals)	**DPDP-R7-2-B-DETAILED-REPORT** (DPDP Rules 2025 r.7(2)(b)(i)-(vi)) Detailed breach report to the Board within 72 hours	**2027-05-13**	199	**CRITICAL**	**290.0**	**High**
CTL-RET-02 Log and traffic-data retention	**DPDP-R6-1-E-LOG-RETENTION** (DPDP Rules 2025 r.6(1)(e)) Retain logs and personal data for one year for breach detection and investigation	**2027-05-13**	199	**CRITICAL**	**290.0**	**High**
CTL-SEC-01 Documented information security programme	**DPDP-S8-5-SAFEGUARDS** (DPDP Act 2023 s.8(5); DPDP Rules 2025 r.6(1)(g)) Take reasonable security safeguards to prevent personal data breach	**2027-05-13**	199	**CRITICAL**	**290.0**	**High**
CTL-SEC-02 Encryption, masking and tokenisation of personal data	**DPDP-R6-1-A-ENCRYPTION** (DPDP Rules 2025 r.6(1)(a)) Data security measures such as encryption, obfuscation, masking or virtual tokens	**2027-05-13**	199	**CRITICAL**	**290.0**	**High**
CTL-SEC-03 Access control over systems holding personal data	**DPDP-R6-1-B-ACCESS-CONTROL** (DPDP Rules 2025 r.6(1)(b)) Control access to computer resources	**2027-05-13**	199	**CRITICAL**	**290.0**	**High**
CTL-SEC-04 Logging and monitoring of ICT systems	**DPDP-R6-1-C-LOGGING** (DPDP Rules 2025 r.6(1)(c)) Visibility on access to personal data through logs, monitoring and review	**2027-05-13**	199	**CRITICAL**	**290.0**	**High**
CTL-SEC-05 Backup and continuity of processing	**DPDP-R6-1-D-CONTINUITY** (DPDP Rules 2025 r.6(1)(d)) Continued processing after compromise, such as by data backups	**2027-05-13**	199	**CRITICAL**	**290.0**	**High**
CTL-TPP-01 Processor and recipient register with written contracts	**DPDP-R6-1-F-PROCESSOR-SECURITY-CLAUSE** (DPDP Rules 2025 r.6(1)(f)) Security safeguards clause in Data Processor contracts	**2027-05-13**	199	**CRITICAL**	**290.0**	**High**
CTL-GOV-02 Privacy compliance programme with accountable owner and staff training	**DPDP-S8-1-ACCOUNTABILITY** (DPDP Act 2023 s.8(1)) Fiduciary is responsible for compliance, including processing by its Data Processors, whatever the contract says	**2027-05-13**	199	**MEDIUM**	**90.6**	**Medium**
CTL-GOV-02 Privacy compliance programme with accountable owner and staff training	**DPDP-S8-4-TOMS** (DPDP Act 2023 s.8(4)) Implement technical and organisational measures for effective observance of the Act	**2027-05-13**	199	**MEDIUM**	**90.6**	**Medium**
CTL-CB-01 Cross-border transfer register and restriction check	**DPDP-S16-R15-TRANSFER** (DPDP Act 2023 s.16(1)-(2); DPDP Rules 2025 r.15) Do not transfer personal data to a notified restricted country; meet any Rule 15 order and stricter laws	**2027-05-13**	199	**MEDIUM**	**72.5**	**Medium**
CTL-DPR-01 Data Principal rights request procedure	**DPDP-R9-CONTACT-IN-RESPONSES** (DPDP Rules 2025 r.9) Mention the privacy contact in every response to a rights communication	**2027-05-13**	199	**MEDIUM**	**72.5**	**Medium**

CONFIDENTIAL DRAFT — NOT VERIFIED

CTL-DPR-01 Data Principal rights request procedure	**DPDP-R14-1-RIGHTS-PUBLISH** (DPDP Rules 2025 r.14(1)(a)-(b), r.14(4); DPDP Act 2023 s.14(1)) Publish how to make rights requests (including nomination) and the identifiers needed	**2027-05-13**	199	**MEDIUM**	**72.5**	**Medium**
CTL-DPR-01 Data Principal rights request procedure	**DPDP-S11-ACCESS** (DPDP Act 2023 s.11(1)(a)-(b)) Provide a summary of personal data, processing and the identities of recipients on request	**2027-05-13**	199	**MEDIUM**	**72.5**	**Medium**
CTL-DPR-01 Data Principal rights request procedure	**DPDP-S12-2-CORRECTION** (DPDP Act 2023 s.12(1)-(2)) Correct, complete and update personal data on request	**2027-05-13**	199	**MEDIUM**	**72.5**	**Medium**
CTL-DPR-01 Data Principal rights request procedure	**DPDP-S12-3-ERASURE-REQUEST** (DPDP Act 2023 s.12(3)) Erase personal data on request unless needed for the purpose or required by law	**2027-05-13**	199	**MEDIUM**	**72.5**	**Medium**
CTL-GRV-02 Published privacy contact point	**DPDP-S6-3-CONSENT-REQUEST** (DPDP Act 2023 s.6(3)) Consent request in plain language, with language option and contact details	**2027-05-13**	199	**MEDIUM**	**72.5**	**Medium**
CTL-GRV-02 Published privacy contact point	**DPDP-S8-9-CONTACT-PUBLISH** (DPDP Act 2023 s.8(9); DPDP Rules 2025 r.9) Prominently publish business contact information of the DPO or a responsible person	**2027-05-13**	199	**MEDIUM**	**72.5**	**Medium**
CTL-GRV-02 Published privacy contact point	**DPDP-R9-CONTACT-IN-RESPONSES** (DPDP Rules 2025 r.9) Mention the privacy contact in every response to a rights communication	**2027-05-13**	199	**MEDIUM**	**72.5**	**Medium**
CTL-GRV-01 Grievance redressal mechanism with published response period	**DPDP-S8-10-GRIEVANCE** (DPDP Act 2023 s.8(10), s.13(1)) Establish an effective grievance redressal mechanism	**2027-05-13**	199	**MEDIUM**	**72.5**	**Medium**
CTL-GRV-01 Grievance redressal mechanism with published response period	**DPDP-R14-3-GRIEVANCE-PERIOD** (DPDP Act 2023 s.13(2); DPDP Rules 2025 r.14(3)) Publish the grievance response period and respond within it (not exceeding 90 days)	**2027-05-13**	199	**MEDIUM**	**72.5**	**Medium**
CTL-NC-01 Notice accompanying or preceding consent requests	**DPDP-S5-1-NOTICE** (DPDP Act 2023 s.5(1)) Give a notice with or before every consent request	**2027-05-13**	199	**MEDIUM**	**72.5**	**Medium**
CTL-NC-01 Notice accompanying or preceding consent requests	**DPDP-R3-NOTICE-FORM** (DPDP Rules 2025 r.3(a)-(c); DPDP Act 2023 s.5(3)) Notice is standalone, itemised, plain-language and offered in English or an Eighth Schedule language	**2027-05-13**	199	**MEDIUM**	**72.5**	**Medium**
CTL-NC-01 Notice accompanying or preceding consent requests	**DPDP-S5-2-LEGACY-NOTICE** (DPDP Act 2023 s.5(2)(a)) Send a notice to Data Principals whose consent predates commencement	**2027-05-13**	199	**MEDIUM**	**72.5**	**Medium**

CONFIDENTIAL DRAFT — NOT VERIFIED

CTL-NC-03 Valid consent capture and consent records	**DPDP-S5-2-LEGACY-NOTICE** (DPDP Act 2023 s.5(2)(a)) Send a notice to Data Principals whose consent predates commencement	**2027-05-13**	199	**MEDIUM**	**72.5**	**Medium**
CTL-NC-03 Valid consent capture and consent records	**DPDP-S6-1-VALID-CONSENT** (DPDP Act 2023 s.6(1)) Consent must be free, specific, informed, unconditional, unambiguous and limited to necessary data	**2027-05-13**	199	**MEDIUM**	**72.5**	**Medium**
CTL-NC-03 Valid consent capture and consent records	**DPDP-S6-3-CONSENT-REQUEST** (DPDP Act 2023 s.6(3)) Consent request in plain language, with language option and contact details	**2027-05-13**	199	**MEDIUM**	**72.5**	**Medium**
CTL-NC-04 Consent withdrawal and processing cessation	**DPDP-S6-4-WITHDRAWAL** (DPDP Act 2023 s.6(4)) Withdrawal of consent as easy as giving it	**2027-05-13**	199	**MEDIUM**	**72.5**	**Medium**
CTL-NC-04 Consent withdrawal and processing cessation	**DPDP-S6-6-CESSATION** (DPDP Act 2023 s.6(6)) Stop processing, and make processors stop, after consent is withdrawn	**2027-05-13**	199	**MEDIUM**	**72.5**	**Medium**
CTL-RET-03 Data accuracy and quality	**DPDP-S8-3-ACCURACY** (DPDP Act 2023 s.8(3)) Ensure completeness, accuracy and consistency of data used for decisions or disclosed	**2027-05-13**	199	**MEDIUM**	**72.5**	**Medium**
CTL-RET-01 Retention and erasure schedule and procedure	**DPDP-S8-7-A-ERASURE** (DPDP Act 2023 s.8(7)(a)) Erase personal data on withdrawal of consent or when the purpose is no longer served	**2027-05-13**	199	**MEDIUM**	**72.5**	**Medium**
CTL-RET-01 Retention and erasure schedule and procedure	**DPDP-S8-7-B-PROCESSOR-ERASURE** (DPDP Act 2023 s.8(7)(b)) Cause Data Processors to erase personal data made available to them	**2027-05-13**	199	**MEDIUM**	**72.5**	**Medium**
CTL-RET-02 Log and traffic-data retention	**DPDP-R8-3-MIN-RETENTION** (DPDP Rules 2025 r.8(3) read with Seventh Schedule) Retain personal data, traffic data and processing logs for at least one year, then erase	**2027-05-13**	199	**MEDIUM**	**72.5**	**Medium**
CTL-RET-01 Retention and erasure schedule and procedure	**DPDP-R8-3-MIN-RETENTION** (DPDP Rules 2025 r.8(3) read with Seventh Schedule) Retain personal data, traffic data and processing logs for at least one year, then erase	**2027-05-13**	199	**MEDIUM**	**72.5**	**Medium**
CTL-RET-03 Data accuracy and quality	**DPDP-S12-2-CORRECTION** (DPDP Act 2023 s.12(1)-(2)) Correct, complete and update personal data on request	**2027-05-13**	199	**MEDIUM**	**72.5**	**Medium**
CTL-RET-01 Retention and erasure schedule and procedure	**DPDP-S12-3-ERASURE-REQUEST** (DPDP Act 2023 s.12(3)) Erase personal data on request unless needed for the purpose or required by law	**2027-05-13**	199	**MEDIUM**	**72.5**	**Medium**

CONFIDENTIAL DRAFT — NOT VERIFIED

CTL-TPP-01 Processor and recipient register with written contracts	**DPDP-S6-6-CESSATION** (DPDP Act 2023 s.6(6)) Stop processing, and make processors stop, after consent is withdrawn	**2027-05-13**	199	**MEDIUM**	**72.5**	**Medium**
CTL-TPP-01 Processor and recipient register with written contracts	**DPDP-S8-2-PROCESSOR-CONTRACT** (DPDP Act 2023 s.8(2)) Engage Data Processors only under a valid contract	**2027-05-13**	199	**MEDIUM**	**72.5**	**Medium**
CTL-TPP-01 Processor and recipient register with written contracts	**DPDP-S8-7-B-PROCESSOR-ERASURE** (DPDP Act 2023 s.8(7)(b)) Cause Data Processors to erase personal data made available to them	**2027-05-13**	199	**MEDIUM**	**72.5**	**Medium**

CONFIDENTIAL
DRAFT — NOT VERIFIED

4. Control Assessment Detail

Detailed on-site assessment logs across thirty-one statutory compliance controls, including evidence verification status and auditor observations.

CTL-GOV-01: Personal data inventory with purposes, grounds and applicability assessment [IMPLEMENTED]

Category: Governance

Guidance: Ask for the record of processing activities. For each activity check that it lists: categories of individuals and personal data, purpose, the ground relied on (consent or a specific legitimate use), systems, recipients and processors, countries where data is stored or accessed, and retention. Check that data collected is limited to what each purpose needs, and that the organisation has recorded which laws and exemptions it believes apply (and why). Sample 3 activities and trace them to the actual systems.

Expected Evidence:
• [UNCLEAR] Processing register / data map (spreadsheet or tool export) with owner and last-review date
• [UNCLEAR] Ground-of-processing mapping per activity
• [UNCLEAR] Written applicability / exemption assessment (role as fiduciary or processor, territorial scope)
• [UNCLEAR] Evidence of a data-minimisation review of forms and data fields

CTL-GOV-02: Privacy compliance programme with accountable owner and staff training [PARTIAL]

Category: Governance

Guidance: Identify the person accountable for data protection and their reporting line. Check for approved privacy and data-handling policies, a compliance calendar, periodic management review, and staff training with attendance records. Check that staff and contractors sign confidentiality undertakings covering personal data.

Expected Evidence:
• [UNCLEAR] Board / management note assigning data-protection responsibility
• [UNCLEAR] Approved privacy and data-handling policies with version history
• [UNCLEAR] Training material and attendance records for the last 12 months
• [UNCLEAR] Signed confidentiality / non-disclosure undertakings (sample of staff and contractors)

CTL-GOV-03: Disclosure authorisation and authority-request handling [NOT IMPLEMENTED]

Category: Governance

Guidance: Check for a written procedure for any disclosure of personal data to third parties and for requests from government agencies or regulators (e.g. CERT-In orders): who can approve, how the basis (consent, contract, legal obligation, written request from a mandated agency) is checked and recorded, and how deadlines in an order are tracked. Review the disclosure / request log for the last 12 months.

Expected Evidence:
• [UNCLEAR] Disclosure and law-enforcement / regulator request procedure
• [UNCLEAR] Disclosure and request log with basis recorded for each entry
• [UNCLEAR] Sample written requests from agencies and responses

CONFIDENTIAL DRAFT — NOT VERIFIED

CTL-NC-01: Notice accompanying or preceding consent requests [NOT ASSESSED]

Category: Notice & Consent

Guidance: Walk through every consent flow (web sign-up, app onboarding, forms, sales demos, recruitment). Check a notice is shown before or with the consent request, that it is standalone and readable on its own, itemises the personal data, states each purpose and the related goods/services/uses, gives a link and the means to withdraw consent, exercise rights and complain to the Data Protection Board, and that it can be read in English or a language of the Eighth Schedule to the Constitution. Check a plan or record of notices sent to existing users whose consent predates commencement.

Expected Evidence:
• [UNCLEAR] Screenshots / copies of each notice in context of the consent flow
• [UNCLEAR] Language versions offered
• [UNCLEAR] Record of notice campaign to existing users (dates, channel, reach)

CTL-NC-02: Published privacy policy on website or app [NOT ASSESSED]

Category: Notice & Consent

Guidance: Open the organisation's website / app and locate the privacy policy. Check it is easily accessible and states practices and policies, types of personal and sensitive data collected, purposes, disclosures, and security practices; and that it is version-controlled and reviewed.

Expected Evidence:
• [UNCLEAR] URL of the published privacy policy and screenshot of how it is reached
• [UNCLEAR] Policy version history and approval record

CTL-NC-03: Valid consent capture and consent records [NOT ASSESSED]

Category: Notice & Consent

Guidance: Inspect consent UI for pre-ticked boxes, bundled consents, consent made a condition for unrelated data, and collection of data not needed for the stated purpose. Check consent requests are in clear and plain language, offer English / Eighth Schedule language access and give the contact of the DPO or an authorised person (DPDP elements - effective from phase 3). SPDI written consent is assessed under CTL-NC-05. Check the organisation can produce, per individual, the notice version shown and the consent record (time, purpose, channel).

Expected Evidence:
• [UNCLEAR] Screenshots of consent UI per flow
• [UNCLEAR] Consent log / database extract with notice version, timestamp, purposes

CTL-NC-05: SPDI collection notice and written consent (SPDI Rules) [NOT ASSESSED]

Category: Notice & Consent

Guidance: SPDI Rules r.5(1) and r.5(3) only (until DPDP phase 3). Where the organisation collects passwords, financial, health, sexual-orientation or biometric data, check that consent for the purpose is obtained in writing (letter, fax or email; the 2011 press note - guidance only - accepts electronic consent), and that the person is made aware of (a) the fact of collection, (b) the purpose, (c) the intended recipients and (d) the name and address of the agency collecting and the agency retaining the information. DPDP notice elements (Eighth Schedule language, Board complaint) are not part of this control.

Expected Evidence:
• [UNCLEAR] Screenshots / copies of SPDI collection points with the notice shown
• [UNCLEAR] Sample written / electronic consents for SPDI
• [UNCLEAR] Name and address of collecting and retaining agencies as shown to the person

CONFIDENTIAL DRAFT — NOT VERIFIED

CTL-NC-04: Consent withdrawal and processing cessation [NOT ASSESSED]

Category: Notice & Consent

Guidance: Compare the steps to withdraw consent with the steps to give it (clicks, channel, login). Trace a test or historical withdrawal: was processing stopped, were processors instructed to stop, and in what time. Check that an option not to provide sensitive data, and its consequences, is offered.

Expected Evidence:
• [UNCLEAR] Withdrawal UI / process description with step count
• [UNCLEAR] Withdrawal log and evidence of instructions to processors
• [UNCLEAR] Documented "reasonable time" target for cessation

CTL-DPR-01: Data Principal rights request procedure [NOT ASSESSED]

Category: Data Principal Rights

Guidance: Check the published means of making requests (access summary, correction, completion, updating, erasure, nomination) and the identifiers required. Check the internal procedure: identity verification, routing, response templates (which must include the privacy contact), and the ability to list all other Data Fiduciaries and Data Processors with whom data was shared. Sample closed requests.

Expected Evidence:
• [UNCLEAR] Published rights-request page / section with channels and required identifiers
• [UNCLEAR] Internal rights-request procedure and templates
• [UNCLEAR] Rights request log with dates and outcomes
• [UNCLEAR] Recipient / processor list usable for access responses

CTL-DPR-02: Route to review and correct information provided [NOT ASSESSED]

Category: Data Principal Rights

Guidance: Check that a person can review the information he or she provided (self-service profile or request channel) and that inaccurate or deficient information is corrected or amended as feasible, including data the person cannot edit directly. Sample correction requests. DPDP-specific rights elements (nomination, recipient lists) belong to CTL-DPR-01, not this control.

Expected Evidence:
• [UNCLEAR] Screenshot of the review / edit route or request channel
• [UNCLEAR] Sample of correction requests and outcomes

CTL-GRV-01: Grievance redressal mechanism with published response period [NOT ASSESSED]

Category: Grievance Redressal

Guidance: Check that a readily available grievance channel is published, a response period is published, and grievances are logged and answered within that period. Review the grievance log for ageing against the period required by each mapped rule. A named individual is NOT required for this control (the SPDI named Grievance Officer is CTL-GRV-03).

Expected Evidence:
• [UNCLEAR] Website / app page showing the grievance channel and response period
• [UNCLEAR] Grievance handling procedure
• [UNCLEAR] Grievance log with receipt and response dates

CONFIDENTIAL DRAFT — NOT VERIFIED

CTL-GRV-02: Published privacy contact point [NOT ASSESSED]

Category: Grievance Redressal

Guidance: Check that business contact information of the DPO (if any) or a person able to answer questions about processing is prominently published on the website / app, and appears in consent requests and rights-request responses.

Expected Evidence:
• [UNCLEAR] Screenshot showing prominence of the contact details
• [UNCLEAR] Sample rights-request responses containing the contact

CTL-GRV-03: Named Grievance Officer published on the website (SPDI Rules) [NOT ASSESSED]

Category: Grievance Redressal

Guidance: SPDI Rules r.5(9) only (until DPDP phase 3). Check that a Grievance Officer has been designated and that his or her name and contact details are published on the website; a role mailbox alone is not enough.

Expected Evidence:
• [UNCLEAR] Designation record of the Grievance Officer
• [UNCLEAR] Screenshot of the website showing the name and contact details

CTL-SEC-01: Documented information security programme [NOT ASSESSED]

Category: Security Safeguards

Guidance: Review the information security policy set and programme: risk assessment, managerial, technical, operational and physical controls proportionate to the information assets, ownership, and review cycle. Note any ISO/IEC 27001 certification (scope and validity) or other standard followed.

Expected Evidence:
• [UNCLEAR] Approved information security policy and supporting standards
• [UNCLEAR] Risk assessment / risk register
• [UNCLEAR] ISO/IEC 27001 certificate and Statement of Applicability, if held

CTL-SEC-02: Encryption, masking and tokenisation of personal data [NOT ASSESSED]

Category: Security Safeguards

Guidance: Check encryption at rest and in transit for systems holding personal data, masking in non-production environments and logs, tokenisation of payment data, and password hashing. Inspect configuration rather than relying on policy alone.

Expected Evidence:
• [UNCLEAR] Encryption configuration screenshots (databases, storage, backups, TLS)
• [UNCLEAR] Data masking approach for test / dev data
• [UNCLEAR] Key management procedure

CONFIDENTIAL DRAFT — NOT VERIFIED

CTL-SEC-03: Access control over systems holding personal data [NOT ASSESSED]

Category: Security Safeguards

Guidance: Check role-based access, least privilege, MFA for administrative and remote access, joiner-mover-leaver process, and periodic access reviews. Sample leavers and check accounts were disabled.

Expected Evidence:
• [UNCLEAR] Access control policy
• [UNCLEAR] User access review records
• [UNCLEAR] MFA configuration evidence
• [UNCLEAR] Leaver sample with deprovisioning timestamps

CTL-SEC-04: Logging and monitoring of ICT systems [NOT ASSESSED]

Category: Security Safeguards

Guidance: Check that logs are enabled on all ICT systems (servers, cloud audit logs, firewall/WAF, IAM/authentication, application, database, VPN, endpoint), capturing successful and failed events, including access to personal data; and that logs are monitored and reviewed. Clock synchronisation is assessed separately (CTL-SEC-07).

Expected Evidence:
• [UNCLEAR] Logging standard and list of log sources
• [UNCLEAR] SIEM / monitoring dashboards and alert review records

CTL-SEC-05: Backup and continuity of processing [NOT ASSESSED]

Category: Security Safeguards

Guidance: Check backups of systems holding personal data, their protection, restore testing, and a continuity / disaster-recovery plan covering loss of confidentiality, integrity or availability.

Expected Evidence:
• [UNCLEAR] Backup policy and schedule
• [UNCLEAR] Last restore test record
• [UNCLEAR] Business continuity / DR plan

CTL-SEC-06: Independent periodic security audit [NOT ASSESSED]

Category: Security Safeguards

Guidance: Check for an independent audit of security practices at least annually and after significant changes to processes or computer resources; check auditor independence and any approval / empanelment claimed, and closure of findings.

Expected Evidence:
• [UNCLEAR] Latest independent audit report and date
• [UNCLEAR] Auditor engagement letter / empanelment evidence
• [UNCLEAR] Findings tracker with closure status

CONFIDENTIAL DRAFT — NOT VERIFIED

CTL-SEC-07: Time synchronisation of ICT system clocks [NOT ASSESSED]

Category: Security Safeguards

Guidance: Check that all ICT system clocks (servers, cloud workloads, network and security devices, logging/SIEM) synchronise to the NTP servers of NIC or NPL or to a source traceable to them; organisations spanning several geographies may use another accurate standard time source that does not deviate from NPL / NIC. Under the non-binding CERT-In FAQs a cloud provider's native time service and UTC are accepted. Synchronisation to an arbitrary public NTP pool is not enough on its own.

Expected Evidence:
• [UNCLEAR] NTP / chrony / cloud time-sync configuration for a sample of 2-3 systems
• [UNCLEAR] Upstream time source and its traceability to NIC / NPL

CTL-BRM-01: Personal data breach intimation procedure (Data Protection Board and affected individuals) [NOT ASSESSED]

Category: Breach Management

Guidance: DPDP only (effective from phase 3; before that assess as readiness). Review the personal data breach procedure: a breach definition matching DPDP s.2(u) with no materiality threshold; intimation to each affected Data Principal without delay with the required contents; initial intimation to the Data Protection Board without delay; the detailed report to the Board within 72 hours of becoming aware (or a longer period allowed on written request) and who requests it; templates, roles and escalation; and the breach register. Do not mark this control not met for CERT-In gaps - those belong to CTL-BRM-02.

Expected Evidence:
• [UNCLEAR] Breach procedure / runbook with the Board and Data Principal timelines
• [UNCLEAR] Notification templates for the Board and affected individuals
• [UNCLEAR] Breach register and records of any intimations made

CTL-BRM-02: CERT-In cyber incident reporting procedure (6 hours) [NOT ASSESSED]

Category: Breach Management

Guidance: Review the incident response procedure for CERT-In: mapping of internal incident categories to the Annexure I types; reporting to CERT-In within 6 hours of noticing or being brought to notice; current CERT-In reporting channels; who decides and reports, including out of hours; the incident register and any reports made. Do not mark this control not met for missing DPDP Board / Data Principal content - that is CTL-BRM-01. Partial first reports and contract-confidentiality points come from the non-binding FAQs and are recommendations only.

Expected Evidence:
• [UNCLEAR] Incident response plan / runbook with the CERT-In 6-hour step and Annexure I mapping
• [UNCLEAR] CERT-In reporting template and contact details
• [UNCLEAR] Incident register for the last 12 months and any CERT-In reports made
• [UNCLEAR] Best practice: tabletop exercise report

CTL-RET-01: Retention and erasure schedule and procedure [NOT ASSESSED]

Category: Processing & Retention

Guidance: Check a retention schedule per data category with triggers (purpose served, consent withdrawn, legal retention), an erasure procedure covering backups and processors, and evidence that erasure actually happens. Check legal-hold exceptions are tied to a specific law.

Expected Evidence:
• [UNCLEAR] Retention schedule
• [UNCLEAR] Erasure procedure and erasure logs / certificates (including from processors)
• [UNCLEAR] List of legal retention requirements relied on

CONFIDENTIAL DRAFT — NOT VERIFIED

CTL-RET-02: Log and traffic-data retention [NOT ASSESSED]

Category: Processing & Retention

Guidance: Check retention settings for logs, traffic data and processing records against each legal minimum that applies (e.g. 180 days rolling for CERT-In, one year for DPDP), where logs are stored (Indian jurisdiction or producible on demand), integrity protection, and erasure after the retention period unless another law requires more.

Expected Evidence:
• [UNCLEAR] Log retention configuration (SIEM, cloud logging, application)
• [UNCLEAR] Storage region evidence for logs
• [UNCLEAR] Log integrity / access-restriction evidence

CTL-RET-03: Data accuracy and quality [NOT ASSESSED]

Category: Processing & Retention

Guidance: Where personal data is used for decisions about individuals or shared with other organisations, check validation at entry, periodic accuracy checks, and a route for individuals to review and correct their data.

Expected Evidence:
• [UNCLEAR] Data quality procedure for decision-making / shared datasets
• [UNCLEAR] Records of correction requests handled

CTL-RET-04: Customer identity and transaction record-keeping [NOT ASSESSED]

Category: Processing & Retention

Guidance: For hosting, cloud, VPN or virtual-asset service lines only: check that customer onboarding captures and validates the required identity and service details, and that these records (and, for virtual assets, KYC and transaction records) are kept for the required period.

Expected Evidence:
• [UNCLEAR] Customer onboarding / KYC procedure
• [UNCLEAR] Sample customer records showing the required fields
• [UNCLEAR] Retention configuration for these records

CTL-TPP-01: Processor and recipient register with written contracts [NOT ASSESSED]

Category: Third-Party Processors

Guidance: Check a register of vendors / processors and other recipients of personal data, with due diligence records, and a written contract for each (click-through terms count). Sample 3 contracts and record which of these clauses are present: reasonable security safeguards (DPDP r.6(1)(f)); stopping processing and erasing data when instructed (supports DPDP s.6(6), s.8(7)(b)); no onward disclosure of SPDI (SPDI r.6(4)); the same level of data protection (SPDI r.7); confidentiality (s.72A exposure). Rate this control on the register and the existence of a contract; a missing clause is a legal gap only under the specific rule that requires it (see each rule's guidance). Instructions-only processing, sub-processor approval, incident notification to the organisation and rights-request assistance are BEST PRACTICE - report them as recommendations and never rate the control not met because they are absent.

Expected Evidence:
• [UNCLEAR] Vendor / processor register
• [UNCLEAR] Signed data processing / sharing agreements (sample)
• [UNCLEAR] Vendor due diligence / security questionnaires

CONFIDENTIAL DRAFT — NOT VERIFIED

CTL-CB-01: Cross-border transfer register and restriction check [NOT ASSESSED]

Category: Cross-Border Transfer

Guidance: Check a list of countries where personal data is stored or accessed (cloud regions, vendors, group companies), the basis for each transfer, and a documented check against any Central Government notification or order restricting transfers and any sectoral localisation rule that applies to the organisation or its clients.

Expected Evidence:
• [UNCLEAR] Transfer register with destination countries
• [UNCLEAR] Record of the last check against government notifications / sectoral rules

CTL-CH-01: Children's and guardian-represented individuals' data safeguards [NOT ASSESSED]

Category: Children's Data

Guidance: Check how the organisation knows whether a user is under 18, how verifiable consent of a parent / lawful guardian is obtained before processing (and how the parent is checked to be an identifiable adult, or the guardian's appointment verified), and that the product does not track, behaviourally monitor, or target advertising at children or process their data in ways likely to harm their well-being.

Expected Evidence:
• [UNCLEAR] Age-gating / age assurance design
• [UNCLEAR] Parental / guardian consent flow and verification records
• [UNCLEAR] Advertising and analytics configuration for child users
• [UNCLEAR] Child well-being risk review

CTL-SDF-01: Significant Data Fiduciary programme [NOT ASSESSED]

Category: Significant Data Fiduciary (SDF)

Guidance: Only where notified as a Significant Data Fiduciary: check appointment of a DPO based in India and responsible to the Board of Directors, appointment of an independent data auditor, periodic (12-monthly) DPIA and audit with report to the Data Protection Board, and due diligence on algorithmic software.

Expected Evidence:
• [UNCLEAR] SDF notification reference
• [UNCLEAR] DPO appointment letter and board reporting evidence
• [UNCLEAR] Independent data auditor engagement
• [UNCLEAR] Latest DPIA and audit reports; evidence of report furnished to the Board
• [UNCLEAR] Algorithmic due diligence records

CTL-REG-01: Regulator point of contact designated and registered [NOT ASSESSED]

Category: Significant Data Fiduciary (SDF)

Guidance: Check that a Point of Contact for CERT-In has been designated, that the details in the Annexure II format were sent to CERT-In, and that there is a process to update them when the person changes.

Expected Evidence:
• [UNCLEAR] PoC designation record
• [UNCLEAR] Copy of submission to CERT-In (Annexure II format) and acknowledgement
• [UNCLEAR] Process for updating PoC details

CONFIDENTIAL DRAFT — NOT VERIFIED

5. Prioritized Remediation Roadmap

The remediation roadmap translates identified gaps into structured, actionable work packages grouped by control. Actions are prioritized by statutory risk score and assigned recommended ownership and deadlines.
Note: Remediation owner, effort, target date, and remediation steps are marked as **Suggested — auditor to confirm**.

Part A: Current Legal Exposure

CTL-GOV-03: Disclosure authorisation and authority-request handling — Priority: High (Risk Score: 290.0)

Target Date (Suggested — auditor to confirm): 2026-12-25 • **Effort (Suggested — auditor to confirm):** Very High • **Owner (Suggested — auditor to confirm):** Data Protection Officer & Legal Counsel

Remediation Steps (Suggested — auditor to confirm):
• No fixed number of hours: the timeframe is whatever the order says. FAQ 38 (non-binding): requests come from an officer not below Deputy Secretary rank - the procedure should verify the requester.
• Applies to any person, not only a body corporate, so it reaches IT service vendors and processors that the 2011 press note places outside SPDI Rules 5 and 6. The words "any person including an intermediary", the "obtains personal information" wording and the intent / knowledge element come from the research summary rather than a verbatim quote - verify the full section text before reporting. An audit cannot establish intent; assess the controls that prevent unauthorised disclosure (approval and logging of disclosures, confidentiality undertakings, training) and report residual exposure rather than an offence.
• Check the disclosure log for a recorded basis per disclosure and, for agency requests, a written request stating the purpose. Disclosure under an order under law is covered by r.6(2). Press note (guidance only): outsourcers acting under contract outside Rule 6.
• Look for SPDI in public repositories, public status pages, shared public links and demo environments.
• Gated on the client receiving SPDI as a service provider. A fiduciary that receives SPDI from another company for its own purposes is also a "third party" - record that manually if relevant. For the client's own disclosures, check the flow-down clause in recipient contracts (processor contract checklist).

Compliance Advisory Services Available:
➔ Executive and employee DPDP awareness training workshop
➔ Privacy risk assessment (good practice)
➔ Virtual / Fractional Data Protection Officer (DPO) retainer service

CTL-GOV-02: Privacy compliance programme with accountable owner and staff training — Priority: High (Risk Score: 181.2)

Target Date (Suggested — auditor to confirm): 2026-12-25 • **Effort (Suggested — auditor to confirm):** Low • **Owner (Suggested — auditor to confirm):** Data Protection Officer & Legal Counsel

Remediation Steps (Suggested — auditor to confirm):
• Applies to any person, not only a body corporate, so it reaches IT service vendors and processors that the 2011 press note places outside SPDI Rules 5 and 6. The words "any person including an intermediary", the "obtains personal information" wording and the intent / knowledge element come from the research summary rather than a verbatim quote - verify the full section text before reporting. An audit cannot establish intent; assess the controls that prevent unauthorised disclosure (approval and logging of disclosures, confidentiality undertakings, training) and report residual exposure rather than an offence.

Compliance Advisory Services Available:
➔ Executive and employee DPDP awareness training workshop
➔ Privacy risk assessment (good practice)
➔ Virtual / Fractional Data Protection Officer (DPO) retainer service

CONFIDENTIAL DRAFT — NOT VERIFIED

Part B: DPDP Readiness

CTL-GOV-02: Privacy compliance programme with accountable owner and staff training — Priority: Critical (Risk Score: 362.5)

Commences: 2027-05-13 (199 days remaining) • **Target Date (Suggested — auditor to confirm):** 2027-05-13 • **Effort (Suggested — auditor to confirm):** Medium • **Owner (Suggested — auditor to confirm):** Data Protection Officer & Legal Counsel

Remediation Steps (Suggested — auditor to confirm):
• s.8(5) (with s.8(1)) survives the s.17(1) exemptions, including the s.17(1)(d) outsourcing carve-out, so this rule does not test s.17(1)(d). The Rule 6(1)(a)-(f) minimum measures are separate rules below. The verbatim opening words of Rule 6(1) were not obtained from any source.
• Deliberately has NO s.17(1)(d) carve-out block: s.17(1) excepts "sub-sections (1) and (5) of section 8" from the exemption [from text, TRAI-hosted copy], so this duty survives for an organisation whose processing is wholly within s.17(1)(d) (in that case it attaches to the surviving s.8(5) / Rule 6 duties). Look for an accountable owner and for any contract term that purports to shift DPDP responsibility to a vendor or to the client's users - such terms do not displace the fiduciary's responsibility. Added by red-team review (finding RT-H05).
• s.8(1) also makes the fiduciary responsible for compliance for processing by it or on its behalf by a processor "irrespective of any agreement to the contrary"; record any reliance on contracts to shift responsibility as an observation here.

Compliance Advisory Services Available:
➔ Executive and employee DPDP awareness training workshop
➔ Privacy risk assessment (good practice)
➔ Virtual / Fractional Data Protection Officer (DPO) retainer service

CTL-BRM-01: Personal data breach intimation procedure (Data Protection Board and affected individuals) — Priority: High (Risk Score: 290.0)

Commences: 2027-05-13 (199 days remaining) • **Target Date (Suggested — auditor to confirm):** 2027-05-13 • **Effort (Suggested — auditor to confirm):** Medium • **Owner (Suggested — auditor to confirm):** CISO / Head of Information Security

Remediation Steps (Suggested — auditor to confirm):
• No materiality or harm threshold: any "personal data breach" as defined in s.2(u) triggers it. The English words on the mode of communication ("through her user account or any mode of communication registered with it") are not confirmed. In an on-site audit before phase 3, test the plan and templates, not past performance.
• This clock runs separately from the CERT-In 6-hour report; do not merge them in the incident plan. The Board's intake channel was not researched - check whether the Board has published one before relying on any address.
• Extension is available only on a written request to the Board; the plan should say who makes that request.

Compliance Advisory Services Available:
➔ Formulating Data Breach Incident Response Protocol & CERT-In 6-hour playbook
➔ Reviewing technical access control and encryption standards (AES-256)
➔ Quarterly security compliance audit & vulnerability verification

CONFIDENTIAL DRAFT — NOT VERIFIED

CTL-RET-02: Log and traffic-data retention — Priority: High (Risk Score: 290.0)

Commences: 2027-05-13 (199 days remaining) • **Target Date (Suggested — auditor to confirm):** 2027-05-13 • **Effort (Suggested — auditor to confirm):** Medium • **Owner (Suggested — auditor to confirm):** Data Protection Officer

Remediation Steps (Suggested — auditor to confirm):
• Separate from, and overlapping with, the Rule 8(3) one-year minimum retention (DPDP-R8-3-MIN-RETENTION) and the CERT-In 180-day log rule. One retention setting of at least one year can satisfy all three if storage location meets CERT-In Direction (iv).
• Applies to every Data Fiduciary, not only Third Schedule classes. Check both the floor (nothing deleted before one year, including where a Data Principal asks for erasure - conflict with s.8(7)/s.12(3) to be resolved by Prem) and the erasure afterwards. Seventh Schedule purposes relate to State use, legal functions/disclosure and SDF assessment. A Jan 2026 MeitY proposal to accelerate Rule 8(3) was not confirmed as notified.

Compliance Advisory Services Available:
➔ Executive and employee DPDP awareness training workshop
➔ Privacy risk assessment (good practice)
➔ Virtual / Fractional Data Protection Officer (DPO) retainer service

CTL-SEC-01: Documented information security programme — Priority: High (Risk Score: 290.0)

Commences: 2027-05-13 (199 days remaining) • **Target Date (Suggested — auditor to confirm):** 2027-05-13 • **Effort (Suggested — auditor to confirm):** High • **Owner (Suggested — auditor to confirm):** CISO / Head of Information Security

Remediation Steps (Suggested — auditor to confirm):
• s.8(5) (with s.8(1)) survives the s.17(1) exemptions, including the s.17(1)(d) outsourcing carve-out, so this rule does not test s.17(1)(d). The Rule 6(1)(a)-(f) minimum measures are separate rules below. The verbatim opening words of Rule 6(1) were not obtained from any source.

Compliance Advisory Services Available:
➔ Formulating Data Breach Incident Response Protocol & CERT-In 6-hour playbook
➔ Reviewing technical access control and encryption standards (AES-256)
➔ Quarterly security compliance audit & vulnerability verification

CTL-SEC-02: Encryption, masking and tokenisation of personal data — Priority: High (Risk Score: 290.0)

Commences: 2027-05-13 (199 days remaining) • **Target Date (Suggested — auditor to confirm):** 2027-05-13 • **Effort (Suggested — auditor to confirm):** High • **Owner (Suggested — auditor to confirm):** CISO / Head of Information Security

Remediation Steps (Suggested — auditor to confirm):
• The Rule says "such as" - encryption is an example, not the only acceptable measure; record what is used and where it is missing.

Compliance Advisory Services Available:
➔ Formulating Data Breach Incident Response Protocol & CERT-In 6-hour playbook
➔ Reviewing technical access control and encryption standards (AES-256)
➔ Quarterly security compliance audit & vulnerability verification

CONFIDENTIAL DRAFT — NOT VERIFIED

CTL-SEC-03: Access control over systems holding personal data — Priority: High (Risk Score: 290.0)

Commences: 2027-05-13 (199 days remaining) • **Target Date (Suggested — auditor to confirm):** 2027-05-13 • **Effort (Suggested — auditor to confirm):** High • **Owner (Suggested — auditor to confirm):** CISO / Head of Information Security

Remediation Steps (Suggested — auditor to confirm):
• Include processors' access to the fiduciary's data (shared admin accounts, vendor support access).

Compliance Advisory Services Available:
➔ Formulating Data Breach Incident Response Protocol & CERT-In 6-hour playbook
➔ Reviewing technical access control and encryption standards (AES-256)
➔ Quarterly security compliance audit & vulnerability verification

CTL-SEC-04: Logging and monitoring of ICT systems — Priority: High (Risk Score: 290.0)

Commences: 2027-05-13 (199 days remaining) • **Target Date (Suggested — auditor to confirm):** 2027-05-13 • **Effort (Suggested — auditor to confirm):** High • **Owner (Suggested — auditor to confirm):** CISO / Head of Information Security

Remediation Steps (Suggested — auditor to confirm):
• Logs that are collected but never reviewed do not meet "monitoring and review".

Compliance Advisory Services Available:
➔ Formulating Data Breach Incident Response Protocol & CERT-In 6-hour playbook
➔ Reviewing technical access control and encryption standards (AES-256)
➔ Quarterly security compliance audit & vulnerability verification

CTL-SEC-05: Backup and continuity of processing — Priority: High (Risk Score: 290.0)

Commences: 2027-05-13 (199 days remaining) • **Target Date (Suggested — auditor to confirm):** 2027-05-13 • **Effort (Suggested — auditor to confirm):** High • **Owner (Suggested — auditor to confirm):** CISO / Head of Information Security

Remediation Steps (Suggested — auditor to confirm):
• An untested backup is weak evidence; ask for the last restore test.

Compliance Advisory Services Available:
➔ Formulating Data Breach Incident Response Protocol & CERT-In 6-hour playbook
➔ Reviewing technical access control and encryption standards (AES-256)
➔ Quarterly security compliance audit & vulnerability verification

CONFIDENTIAL DRAFT — NOT VERIFIED

CTL-TPP-01: Processor and recipient register with written contracts — Priority: High (Risk Score: 290.0)

Commences: 2027-05-13 (199 days remaining) • **Target Date (Suggested — auditor to confirm):** 2027-05-13 • **Effort (Suggested — auditor to confirm):** High • **Owner (Suggested — auditor to confirm):** Legal & Procurement Lead

Remediation Steps (Suggested — auditor to confirm):
• Use the processor contract document checklist. Click-through cloud terms count as contracts; check they contain a security commitment.
• The Gazette text says withdrawal "under sub-section (5)" although withdrawal is granted by s.6(4); read it as referring to the s.6(4) withdrawal. If the client uses no processors, assess only its own cessation (CTL-TPP-01 then needs only a nil vendor register). Withdrawal does not affect the legality of earlier processing (s.6(5)).
• The Act prescribes no mandatory clauses; it requires only a "valid contract". Rate this rule on the register and the existence of a valid contract for each processor (CTL-TPP-01 is rated on that basis; best-practice clauses never make it fail). Contract content beyond that is grounded in s.8(1) (fiduciary remains responsible irrespective of any agreement), r.6(1)(f) (security clause), s.6(6) and s.8(7)(b); anything further (e.g. breach notice to the fiduciary) is best practice and should be reported as such. Note the words "for any activity related to offering of goods or services to Data Principals".g. HR) processors.
• Look for an erasure clause in contracts and erasure confirmations from vendors at off-boarding.

Compliance Advisory Services Available:
➔ Drafting Data Processing Agreements (DPA) with statutory processor clauses
➔ Conducting vendor privacy due diligence and international transfer audit

CTL-CB-01: Cross-border transfer register and restriction check — Priority: Medium (Risk Score: 72.5)

Commences: 2027-05-13 (199 days remaining) • **Target Date (Suggested — auditor to confirm):** 2027-05-13 • **Effort (Suggested — auditor to confirm):** Low • **Owner (Suggested — auditor to confirm):** Legal & Procurement Lead

Remediation Steps (Suggested — auditor to confirm):
• Negative-list model: there is no adequacy, standard-contract or transfer-mechanism requirement in the Act. No s.16(1) notification and no Rule 15 order was found in the research (as at Oct 2026) - the auditor must re-check before the visit. If none exists, the finding is about the register and monitoring process, not a breach. Sectoral localisation (e.g. for a fintech client's data) is preserved by s.16(2).

Compliance Advisory Services Available:
➔ Drafting Data Processing Agreements (DPA) with statutory processor clauses
➔ Conducting vendor privacy due diligence and international transfer audit

CONFIDENTIAL DRAFT — NOT VERIFIED

CTL-DPR-01: Data Principal rights request procedure — Priority: Medium (Risk Score: 72.5)

Commences: 2027-05-13 (199 days remaining) • **Target Date (Suggested — auditor to confirm):** 2027-05-13 • **Effort (Suggested — auditor to confirm):** Very High • **Owner (Suggested — auditor to confirm):** Data Protection Officer & Product Lead

Remediation Steps (Suggested — auditor to confirm):
• Check response templates and a sample of sent responses.
• s.14 grants the nomination right "in such manner as may be prescribed"; r.14(4) lets the Data Principal nominate "using the means and furnishing the particulars required by such Data Fiduciary". The duty to offer a nomination route is read from these words.
• s.11(2) excludes clauses (b) and (c) for sharing with a fiduciary authorised by law on a written request for prevention/detection/investigation of offences or cyber incidents. The Act has no portability right and no right to object to automated decisions - do not import them. Can be disapplied for notified fiduciaries under s.17(3); none checked.
• Data Principals must furnish only verifiably authentic information (s.15(e)); the fiduciary may verify before correcting.
• Interaction with the Rule 8(3) one-year minimum retention is unresolved.

Compliance Advisory Services Available:
➔ Drafting Data Principal Rights Handling Manual (access, correction, erasure)
➔ Setting up statutory Grievance Redressal Mechanism & escalation SLA

CTL-GRV-01: Grievance redressal mechanism with published response period — Priority: Medium (Risk Score: 72.5)

Commences: 2027-05-13 (199 days remaining) • **Target Date (Suggested — auditor to confirm):** 2027-05-13 • **Effort (Suggested — auditor to confirm):** Medium • **Owner (Suggested — auditor to confirm):** Data Protection Officer & Customer Support Lead

Remediation Steps (Suggested — auditor to confirm):
• Data Principals must exhaust this mechanism before approaching the Board (s.13(3)), so a missing mechanism also affects their route to the Board.
• Ninety days is a ceiling, not a target; the published period must itself be "reasonable". Before phase 3 the SPDI one-month grievance rule (SPDI-R5-9) applies instead; clients moving from the SPDI one-month process need not lengthen it.

Compliance Advisory Services Available:
➔ Drafting Data Principal Rights Handling Manual (access, correction, erasure)
➔ Setting up statutory Grievance Redressal Mechanism & escalation SLA

CTL-GRV-02: Published privacy contact point — Priority: Medium (Risk Score: 72.5)

Commences: 2027-05-13 (199 days remaining) • **Target Date (Suggested — auditor to confirm):** 2027-05-13 • **Effort (Suggested — auditor to confirm):** Medium • **Owner (Suggested — auditor to confirm):** Data Protection Officer & Customer Support Lead

Remediation Steps (Suggested — auditor to confirm):
• A DPO is mandatory only for a Significant Data Fiduciary (s.10(2)(a)); others name an authorised person.
• A generic info@ address buried in the footer of the terms page is unlikely to be "prominent".
• Check response templates and a sample of sent responses.

Compliance Advisory Services Available:
➔ Drafting Data Principal Rights Handling Manual (access, correction, erasure)
➔ Setting up statutory Grievance Redressal Mechanism & escalation SLA

CONFIDENTIAL DRAFT — NOT VERIFIED

CTL-NC-01: Notice accompanying or preceding consent requests — Priority: Medium (Risk Score: 72.5)

Commences: 2027-05-13 (199 days remaining) • **Target Date (Suggested — auditor to confirm):** 2027-05-13 • **Effort (Suggested — auditor to confirm):** High • **Owner (Suggested — auditor to confirm):** Data Protection Officer & Product Lead

Remediation Steps (Suggested — auditor to confirm):
• Use the DPDP notice document checklist. Under s.6(10) the fiduciary bears the burden of proving that notice was given and consent obtained, so the absence of notice records weakens the position even if a notice exists. s.17(3) allows the Government to exempt notified fiduciaries (including startups) from s.5; no such notification was checked in the research - ask the client and record the reference if claimed.
• Auditable checks: standalone (not only incorporated by reference into terms of service); data itemised rather than described only by broad category; each purpose mapped to a good, service or use; link given; withdrawal, rights and Board-complaint means described; language option offered. Whether every Eighth Schedule language must be offered, or the option of at least one, is an interpretive point.
• By s.1(2), "commencement of this Act" in s.5(2) means commencement of s.5 itself (phase 3). For an audit before that date, record a readiness finding: is there a plan, user list and template for the legacy-notice campaign? The Act gives no fixed deadline ("as soon as it is reasonably practicable").

Compliance Advisory Services Available:
➔ Drafting customized multilingual DPDP Privacy Notice
➔ Formulating granular consent architecture and itemized notices
➔ Designing consent withdrawal workflow and preference center

CTL-NC-03: Valid consent capture and consent records — Priority: Medium (Risk Score: 72.5)

Commences: 2027-05-13 (199 days remaining) • **Target Date (Suggested — auditor to confirm):** 2027-05-13 • **Effort (Suggested — auditor to confirm):** High • **Owner (Suggested — auditor to confirm):** Data Protection Officer & Product Lead

Remediation Steps (Suggested — auditor to confirm):
• By s.1(2), "commencement of this Act" in s.5(2) means commencement of s.5 itself (phase 3). For an audit before that date, record a readiness finding: is there a plan, user list and template for the legacy-notice campaign? The Act gives no fixed deadline ("as soon as it is reasonably practicable").
• Red flags: pre-ticked boxes, a single "I agree" covering unrelated purposes, consent made a condition of service for data not needed for it, collection of data beyond the purpose (the Act's illustration: a telemedicine app may not access contacts). Clauses waiving the right to complain to the Board are invalid (s.6(2) illustration). Keep notice and consent records: s.6(10) puts the burden of proof on the fiduciary.
• A DPO is mandatory only for a Significant Data Fiduciary (s.10(2)(a)); others name an authorised person.

Compliance Advisory Services Available:
➔ Drafting customized multilingual DPDP Privacy Notice
➔ Formulating granular consent architecture and itemized notices
➔ Designing consent withdrawal workflow and preference center

CONFIDENTIAL DRAFT — NOT VERIFIED

CTL-NC-04: Consent withdrawal and processing cessation — Priority: Medium (Risk Score: 72.5)

Commences: 2027-05-13 (199 days remaining) • **Target Date (Suggested — auditor to confirm):** 2027-05-13 • **Effort (Suggested — auditor to confirm):** High • **Owner (Suggested — auditor to confirm):** Data Protection Officer & Product Lead

Remediation Steps (Suggested — auditor to confirm):
• Compare channels and step counts. Consent by one click online but withdrawal only by written letter or email to an unpublished address is a likely gap. Rule 3(c)(i) requires the notice to describe the withdrawal means.
• The Gazette text says withdrawal "under sub-section (5)" although withdrawal is granted by s.6(4); read it as referring to the s.6(4) withdrawal. If the client uses no processors, assess only its own cessation (CTL-TPP-01 then needs only a nil vendor register). Withdrawal does not affect the legality of earlier processing (s.6(5)).

Compliance Advisory Services Available:
➔ Drafting customized multilingual DPDP Privacy Notice
➔ Formulating granular consent architecture and itemized notices
➔ Designing consent withdrawal workflow and preference center

CTL-RET-01: Retention and erasure schedule and procedure — Priority: Medium (Risk Score: 72.5)

Commences: 2027-05-13 (199 days remaining) • **Target Date (Suggested — auditor to confirm):** 2027-05-13 • **Effort (Suggested — auditor to confirm):** High • **Owner (Suggested — auditor to confirm):** Data Protection Officer

Remediation Steps (Suggested — auditor to confirm):
• s.8(8) deems the purpose no longer served after a prescribed period of non-engagement; the Rules prescribe periods only for Third Schedule classes (large e-commerce, online gaming and social media platforms - out of V1 segment). Other fiduciaries rely on s.8(7) judgement. Must be reconciled with the Rule 8(3) one-year minimum retention. Can be disapplied for notified fiduciaries under s.17(3); none checked.
• Look for an erasure clause in contracts and erasure confirmations from vendors at off-boarding.
• Applies to every Data Fiduciary, not only Third Schedule classes. Check both the floor (nothing deleted before one year, including where a Data Principal asks for erasure - conflict with s.8(7)/s.12(3) to be resolved by Prem) and the erasure afterwards. Seventh Schedule purposes relate to State use, legal functions/disclosure and SDF assessment. A Jan 2026 MeitY proposal to accelerate Rule 8(3) was not confirmed as notified.
• Interaction with the Rule 8(3) one-year minimum retention is unresolved.

Compliance Advisory Services Available:
➔ Executive and employee DPDP awareness training workshop
➔ Privacy risk assessment (good practice)
➔ Virtual / Fractional Data Protection Officer (DPO) retainer service

CTL-RET-03: Data accuracy and quality — Priority: Medium (Risk Score: 72.5)

Commences: 2027-05-13 (199 days remaining) • **Target Date (Suggested — auditor to confirm):** 2027-05-13 • **Effort (Suggested — auditor to confirm):** Medium • **Owner (Suggested — auditor to confirm):** Data Protection Officer

Remediation Steps (Suggested — auditor to confirm):
• Can be disapplied for notified fiduciaries under s.17(3); none checked.
• Data Principals must furnish only verifiably authentic information (s.15(e)); the fiduciary may verify before correcting.

Compliance Advisory Services Available:
➔ Executive and employee DPDP awareness training workshop
➔ Privacy risk assessment (good practice)
➔ Virtual / Fractional Data Protection Officer (DPO) retainer service

CONFIDENTIAL DRAFT — NOT VERIFIED

6. Audit Log Summary & Cryptographic Integrity

All audit interactions, questionnaire entries, control assessments, and walk-through findings are immutably chained using SHA-256 cryptographic hashes. The integrity of the audit ledger is validated below:

Audit Ledger Metric	Verification Value / Ledger State
Cryptographic Chain Status:	**CHAIN VALIDATED**
Total Logged Audit Events:	**33 events** (recorded with immutable SHA-256 sequence)
Initial Event Timestamp (UTC):	2026-10-26 14:29:24
Final Event Timestamp (UTC):	2026-10-26 14:29:43
Session Vault Commitment Hash:	aa0d17d71d9811b1e1f30f7b35e4638b0c7dedc5695e04cec0a4bf7736a07702
Sign-Off Finalization:	Completed on **2026-10-26T14:29:43.025959+00:00** by **Prem Singh**

CONFIDENTIAL DRAFT — NOT VERIFIED

7. Statutory Disclaimers & Sign-Off

LEGAL NATURE OF ASSESSMENT: This compliance review was prepared by Prem Singh, WebCompliance.in. It constitutes a technical and operational gap analysis conducted by WebCompliance.in. It does not constitute formal legal advice or a binding legal opinion. The findings, gap scores, and recommended roadmap represent professional evaluations based on the facts, representations, and evidence furnished by the client organisation during on-site audit sessions.

REGULATORY CITATIONS & STATUTORY UPDATES: Compliance citations reference the Digital Personal Data Protection Act, 2023, Information Technology Act, 2000, and subordinate rules in force as of the audit date. Because subordinate rules and guidelines under the DPDP Act are evolving, all rule requirements marked as DRAFT must be re-verified against final notifications published by the Ministry of Electronics and Information Technology (MeitY).

LIMITATION OF LIABILITY: Implementation of the remediation roadmap does not guarantee immunity from inquiry, investigation, or adjudication by the Data Protection Board of India or CERT-In.

Auditor Name:	Prem Singh
Title / Role:	Lead Privacy & Data Protection Compliance Auditor
Audit Sign-Off Date:	2026-10-26
Cryptographic Signature Hash:	aa0d17d71d9811b1e1f30f7b35e4638b0c7dedc5695e04cec0a4bf7736a07702
Auditor Signature / Seal:	_____

CONFIDENTIAL
DRAFT — NOT VERIFIED