SRIDA IT PROFESSIONAL REFERENCE PUBLICATION

DPDP Act, 2023

& Digital Personal Data Protection Rules, 2025

Requirements, Implementation Guidance & Audit Testing Procedures

DOCUMENT ID	VERSION	STATUS
SRIDA-DPDP-RTP-001	1.1	Final — Approved for Publication

Rajendra Bodda
Chief Information Security Officer (CISO)
Srida IT · 2026

Independent professional guidance.
Not legal advice. Not a Government publication.



Digital Personal Data Protection Act, 2023 & DPDP Rules, 2025

Requirements, Implementation Guidance & Audit Testing Procedures

SAMPLE

Prepared by

Rajendra Bodda

Chief Information Security Officer (CISO)

Published by Srida IT

SRIDA-DPDP-RTP-001 · Version 1.1 · October 2026

This publication is an independently developed professional guidance document prepared by Srida IT. It is not legal advice; it is not an official publication of the Government of India, the Ministry of Electronics and Information Technology or the Data Protection Board of India; it does not replace the official text of the Digital Personal Data Protection Act, 2023 or the Digital Personal Data Protection Rules, 2025; and it does not confer any certification, approval or statutory status.

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-dpdpa · © 2026 Srida IT

Document Information and Control

Field	Value
Document title	Digital Personal Data Protection Act, 2023 & DPDP Rules, 2025
Subtitle	Requirements, Implementation Guidance & Audit Testing Procedures
Document identifier	SRIDA-DPDP-RTP-001
Version	1.1
Status	Final — Approved for Publication
Classification	Srida IT Professional Reference Publication
Author	Rajendra Bodda, Chief Information Security Officer (CISO)
Publisher	Srida IT
Publication year	2026
Issue date	October 2026
Legal sources	Digital Personal Data Protection Act, 2023 (No. 22 of 2023); Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), 13 November 2025, as corrected by G.S.R. 892(E); commencement notification G.S.R. 843(E)
Law stated as at	25 October 2026
Requirement spine	Srida IT Stage 4A.2 spine (corrections of 25 October 2026): 221 validated requirements, 103 canonical controls, open legal questions G1–G8
Companion publications	SRIDA-ISMS-27001-RTP-001; SRIDA-AIMS-42001-RTP-001; SRIDA-AIS-27090-RTP-001
Next review	On any amendment to the Act or Rules, any relevant notification, Board guidance or court decision; and at least annually

SAMPLE

Version history

Version	Date	Author	Description of change
1.0	October 2026	Rajendra Bodda	First published edition, approved for publication.
1.1	October 2026	Rajendra Bodda	Requirement spine corrected to Stage 4A.2: four controls re-pointed from superseded requirement IDs to the split requirements; G7 and G2 wording aligned with the Pre-Stage 4 Gate matrix; two G.S.R. 892(E) citations corrected. No legal position changed.

Approval

Role	Name	Date
Approved for publication	Rajendra Bodda, Chief Information Security Officer (CISO)	25 October 2026

Distribution

Released for publication by Srida IT. Distribution and use are subject to the permitted-use terms in the Copyright, Legal and Usage Notices.

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-dpdpa · © 2026 Srida IT

Table of Contents

Part I Foundations 17

Chapter 1 Introduction to the DPDP Act, 2023 and DPDP Rules, 2025 18
Chapter 2 Structure of the Act and Rules and the Commencement Timeline 22
Chapter 3 Roles, Scope and Core Concepts 28
Chapter 4 DPDPA and Related Laws, Standards and Frameworks 33
Chapter 5 Terminology, Definitions and Abbreviations 39
Chapter 6 How to Use This Manual 44
Chapter 7 Audit Methodology, Evidence, Sampling and Open Legal Questions 48

Part II Requirements of the Act and Rules 55

Chapter 8 Application, Commencement and Grounds 56
R-01 Commencement and phased application 57
R-02 Scope, applicability and key definitions 62
R-03 Grounds for processing personal data 69
Chapter 9 Notice, Consent and Legitimate Uses 74
R-04 Notice to the Data Principal 75
R-05 Consent 81
R-06 Consent Managers 87
R-07 Certain legitimate uses and State processing standards 94
Chapter 10 General Obligations of Data Fiduciaries 100
R-08 Accountability of the Data Fiduciary and use of Data Processors 101
R-09 Completeness, accuracy and consistency of personal data 107
R-10 Reasonable security safeguards 111
R-11 Personal data breach intimation 116
R-12 Erasure and retention of personal data 122
R-13 Contact information and grievance redressal 128
Chapter 11 Children and Persons with Disability 133
R-14 Processing personal data of children and persons with disability 134
Chapter 12 Significant Data Fiduciaries 140
R-15 Significant Data Fiduciaries 141
Chapter 13 Rights and Duties of Data Principals 146
R-16 Right to access information about personal data 147
R-17 Right to correction and erasure 153
R-18 Right to nominate 158
R-19 Duties of Data Principals 162
Chapter 14 Cross-Border Processing, Exemptions and Government Information 166
R-20 Processing of personal data outside India 167
R-21 Exemptions 172
R-22 Information to the Central Government 178
Chapter 15 The Data Protection Board, Enforcement and Penalties 183
R-23 The Data Protection Board: complaints and inquiry 184
R-24 Voluntary undertakings, appeals and alternate dispute resolution 190
R-25 Penalties and adjudication 194

Part III Srida IT Canonical Controls 199

Chapter 16 Governance, Applicability, Inventory and Records 200
CTL-GOV-01 Fiduciary accountability and appropriate technical and organisational measures 201
CTL-GOV-02 Privacy lead designation and operating mandate 205
CTL-GOV-03 Published business contact for Data Principal questions (Rule 9) and its inclusion in every rights response 209

SAMPLE

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-dpdpa · © 2026 Srida IT

CTL-APP-01 DPDPA scope and applicability profile 213
CTL-APP-02 Fiduciary / processor role determination per processing activity 217
CTL-APP-03 Obligation commencement calendar and legal-interplay register 221
CTL-INV-01 Processing activity inventory 225
CTL-INV-02 Recipient and sharing register able to answer per Data Principal 229
CTL-INV-03 Collection-point and tracker register 233
CTL-REG-01 Intake, legal hold and response file for Data Protection Board complaints, inquiries and information requirements 237
CTL-REG-02 Compliance with Board directions, urgent breach directions and interim orders; representations for modification 241
CTL-REG-03 Voluntary undertakings under s.32 — governance of the offer and adherence to accepted terms 245
CTL-REG-04 Appeal readiness — sixty-day appeal to the Appellate Tribunal (TDSAT) 249
CTL-REG-05 Government information calls under s.36 and Rule 23, including authority verification and non-disclosure directions 253
CTL-REG-06 Blocking directions under s.37 — intermediary compliance and fiduciary hearing readiness 257
CTL-TRN-01 Role-based DPDPA training and awareness with completion records 261
CTL-TRN-02 Competence of the roles the law depends on, tested by recognition rather than recall 265

Chapter 17 Notice, Consent and Consent Managers 269

CTL-NOT-01 Standalone, itemised notice accompanies or precedes every consent request 270
CTL-NOT-02 Working notice links for withdrawal, rights and Board complaint (Rule 3(c)) 274
CTL-NOT-03 Plain language, English/Eighth Schedule language option and contact details on notices and consent requests 277
CTL-NOT-04 Legacy consent notice (consents given before s.5 commencement) 281
CTL-CON-01 Valid consent capture (free, specific, informed, unconditional, unambiguous, clear affirmative action) 284
CTL-CON-02 Consent limited to necessary personal data and free of infringing terms 287
CTL-CON-03 Withdrawal of consent with comparable ease 290
CTL-CON-04 Cease processing on withdrawal and cause Data Processors to cease 293
CTL-CON-05 Proof of notice and consent (consent ledger linked to notice versions) 296
CTL-CMG-01 Honour consent given, managed, reviewed or withdrawn through a registered Consent Manager 299
CTL-CMG-02 Consent Manager registration: eligibility conditions, application and continued fulfilment 302
CTL-CMG-03 Consent Manager accountability to Data Principals, fiduciary capacity and conflict-of-interest management 306
CTL-CMG-04 Consent Manager platform: direct and routed consent, and website/app as primary access 309
CTL-CMG-05 Consent Manager data-blind sharing and reasonable security safeguards 312
CTL-CMG-06 Consent Manager records of consents, notices and sharing; Data Principal access; seven-year retention 315
CTL-CMG-07 Consent Manager does not sub-contract or assign its obligations 318
CTL-CMG-08 Consent Manager ownership, management and shareholding disclosures 321
CTL-CMG-09 Consent Manager audit mechanisms, reporting to the Board and response to Board information calls 324
CTL-CMG-10 Prior Board approval for transfer of control of a Consent Manager 327

Chapter 18 Legitimate Uses, Children and Exemptions 330

CTL-LGU-01 Lawful purpose and lawful ground (consent or a specific s.7 use) determined before processing 331
CTL-LGU-02 Reliance on voluntary provision (s.7(a)) evidenced and ended on indication of non-consent 335
CTL-LGU-03 Employment legitimate use (s.7(i)) kept within its boundaries 339
CTL-LGU-04 Legal disclosure to the State (s.7(d)) and compliance with judgments, decrees or orders (s.7(e)) 343
CTL-LGU-05 Medical emergency, epidemic and disaster processing (s.7(f)–(h)) invoked, bounded and wound down 347
CTL-LGU-06 State and instrumentality processing under s.7(b)–(c), with Second Schedule intimation for s.7(b) 351
CTL-CHI-01 Determining whether a Data Principal is a child (under 18) 355
CTL-CHI-02 Verifiable parental consent with Rule 10 due diligence 359
CTL-CHI-03 Verifiable consent of lawful guardian of a person with disability (Rule 11 verification) 363
CTL-CHI-04 No processing likely to cause detrimental effect on a child's well-being 367
CTL-CHI-05 No tracking, behavioural monitoring or targeted advertising directed at children 370
CTL-CHI-06 Fourth Schedule class and purpose exemptions relied on only within their conditions 374
CTL-EXM-01 Register of s.17(1) partial exemptions relied on, with surviving obligations honoured 378
CTL-EXM-02 Monitoring of notified exemptions; no self-granted exemption (s.17(2)(a), s.17(3), s.17(5)) 382
CTL-EXM-03 Research, archiving or statistical processing exemption — Second Schedule standards (Rule 16) 386
CTL-EXM-04 State processing under s.7(b): Second Schedule standards, intimation, and s.17(4) carve-outs 390

Chapter 19 Security Safeguards, Breach, Processors and Data Quality 394

CTL-DQ-01 Completeness, accuracy and consistency of personal data used for decisions or disclosed to another fiduciary 395
CTL-SEC-01 Reasonable security safeguards baseline covering all personal data in possession or control, including processors 399
CTL-SEC-02 Data security measures — encryption, obfuscation, masking or virtual tokens 403
CTL-SEC-03 Access control to computer resources used by the fiduciary and its processors 407

SAMPLE

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-dpdpa · © 2026 Srida IT

CHAPTER 1

Introduction to the DPDP Act, 2023 and DPDP Rules, 2025

For most of the past two decades, the protection of personal data in India rested on a narrow statutory base. Section 43A of the Information Technology Act, 2000 and the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 required body corporates to maintain reasonable security practices for a defined class of "sensitive personal data or information", and allowed compensation where negligence caused wrongful loss or gain. Sectoral regulators added their own expectations for banks, insurers, securities intermediaries, telecom operators and health providers. There was no single law that told every organisation, in every sector, what it could and could not do with personal data, what it owed to the individuals concerned, and who would hold it to account.

The Digital Personal Data Protection Act, 2023 (No. 22 of 2023) fills that gap. It received the assent of the President on 11 August 2023 and was published in the Gazette of India, Extraordinary, Part II, Section 1, on the same date. Its long title describes its purpose as providing for the processing of digital personal data in a manner that recognises both the right of individuals to protect their personal data and the need to process such data for lawful purposes. The Digital Personal Data Protection Rules, 2025 were notified by the Ministry of Electronics and Information Technology as G.S.R. 846(E) on 13 November 2025, after a draft (G.S.R. 02(E)) was published for consultation on 3 January 2025. A separate notification of the same date, G.S.R. 843(E), appointed the dates on which the sections of the Act come into force.

This chapter introduces the law, explains its design, sets out where it stands in October 2026, and describes the purpose, scope and limits of this manual.

1.1 What the law does

The Act regulates a single activity: the processing of digital personal data. It does not regulate data in general, it does not create a category of "sensitive" personal data, and it does not apply to personal data that has never been in digital form. Within that boundary, it is built around a small number of design choices that shape every obligation in Parts II and III of this manual.

- **Two lawful grounds, and only two.** Under s.4(1), personal data may be processed only for a lawful purpose and either with the consent of the Data Principal or for "certain legitimate uses". The legitimate uses are those listed in s.7(a)–(i). There is no general "legitimate interests" ground, no general "contract" ground and no open-ended "legal obligation" ground of the kind found in other regimes.
- **Notice before consent.** Every request for consent must be accompanied or preceded by a notice (s.5(1)), whose manner is prescribed by Rule 3. Consent must be free, specific, informed, unconditional and unambiguous, with a clear affirmative action (s.6(1)), and withdrawable with comparable ease (s.6(4)).
- **Accountability rests on the Data Fiduciary.** The person who determines the purpose and means of processing is responsible for compliance, including for processing undertaken on its behalf by a Data Processor, "irrespective of any agreement to the contrary" (s.8(1)).
- **A short, specific security and breach regime.** Section 8(5) requires reasonable security safeguards to prevent personal data breach; Rule 6 sets out the minimum safeguards. Section 8(6) and Rule 7 require intimation of every personal data breach to the Board and to each affected Data Principal, with no harm threshold.
- **Erasure as the default end state.** Personal data is to be erased when consent is withdrawn or the specified purpose is no longer served, unless retention is necessary for compliance with law (s.8(7)), subject to the retention provisions of Rule 8.
- **Enhanced protection for children and certain persons with disability.** Verifiable consent of the parent or lawful guardian is required (s.9(1); Rules 10–11), and tracking, behavioural monitoring and targeted advertising directed at children are prohibited (s.9(3)), subject to the Fourth Schedule exemptions (Rule 12).
- **A tier of Significant Data Fiduciaries.** The Central Government may notify a Data Fiduciary or class of Data Fiduciaries as Significant Data Fiduciaries (s.10(1)). Only those notified carry the additional duties: a Data Protection Officer, an independent data auditor, periodic Data Protection Impact Assessment and audit (s.10(2); Rule 13).
- **Rights and duties of Data Principals.** Chapter III gives rights of access, correction and erasure, grievance redressal and nomination (ss.11–14), and places duties on Data Principals (s.15).
- **A permissive cross-border model.** Transfers outside India are permitted except to a country or territory that the Central Government restricts by notification (s.16(1)), without displacing any law that provides a higher degree of protection or restriction (s.16(2)).
- **A digital-by-design regulator with civil penalties.** The Data Protection Board of India (ss.18–28) inquires into breaches and may impose monetary penalties up to the amounts in the Schedule to the Act (s.33). Appeals lie to the Telecom Disputes Settlement and

SAMPLE

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-dpdpa · © 2026 Srida IT

Appellate Tribunal (s.29). The Act creates no criminal offences.

1.2 Where the law stands in October 2026

The Act does not come into force all at once. Section 1(2) allows different dates for different provisions, and G.S.R. 843(E) and Rule 1 of the Rules use that power to create three phases. Chapter 2 sets out the detail and the qualifications that attach to each date. In summary:

Table 1-1. The three commencement phases at a glance

Phase	Date	What comes into force	Status at October 2026
1	13 Nov 2025	Act s.1(2), s.2, ss.18–26, s.35, ss.38–43, s.44(1) and (3); Rules 1, 2 and 17–21. Definitions, the establishment and constitution of the Board, rule-making and miscellaneous provisions.	In force
2	13 Nov 2026	Act s.6(9) and s.27(1)(d); Rule 4 and the First Schedule. Registration and obligations of Consent Managers.	Not yet in force; weeks away
3	13 May 2027	Act ss.3–5, s.6(1)–(8) and (10), ss.7–17, s.27 except (1)(d), ss.28–34, s.36, s.37 and s.44(2); Rules 3, 5–16, 22 and 23. Almost every Data Fiduciary obligation, the Board's inquiry and penalty powers, and the omission of s.43A of the IT Act.	Not yet in force

Each date carries a ±1 day qualification arising from how the date of publication of the notifications is read; see Chapter 2.

The practical consequence for organisations is that the substantive obligations of a Data Fiduciary are not yet enforceable, but the time remaining to prepare is short. The definitions in s.2 are already in force, the Board can already be constituted and staffed, and the Rules that will govern notice, security, breach intimation, retention, children's data, rights and Significant Data Fiduciaries are already published in final form. There is no longer any reason to describe the Rules as "draft" or to wait for "final Rules".

> **Readiness, not non-compliance**
>
> Until 13 May 2027 (±1 day), a gap against an obligation that commences on that date is a readiness gap, not a current breach of the Act. This manual's testing procedures can be performed now, but findings against Phase 3 provisions are to be reported as readiness findings. Chapter 7 explains how.

1.3 Who is affected

The Act applies to any "person" that processes digital personal data within its territorial scope (s.3, from 13 May 2027). "Person" is defined in s.2(s) to include individuals, Hindu undivided families, companies, firms, associations of persons, the State and every artificial juristic person. There is no size threshold, no turnover threshold and no sector exclusion for private organisations. A 52-person logistics firm in Hyderabad that keeps employee records in a payroll system, a 600-employee fintech in Bengaluru, a hospital chain, a school and a government department are all within scope for the processing they carry out, subject to the exemptions in s.17.

The intensity of the obligations, however, varies with role and circumstance:

- Every **Data Fiduciary** carries the Chapter II obligations: lawful ground, notice, consent, accountability for processors, security safeguards, breach intimation, retention and erasure, contact information and grievance redressal.
- **Data Processors** are reached principally through the valid contract required by s.8(2) and the Data Fiduciary's accountability under s.8(1) and s.8(5); Rule 6(1)(f) requires the contract to provide for reasonable security safeguards.
- Fiduciaries that process the data of **children** or of **persons with disability who have a lawful guardian** carry the additional duties in s.9 and Rules 10–12.
- Only a **Significant Data Fiduciary**, once notified by the Central Government, carries the s.10(2) duties and Rule 13.
- **Consent Managers** are a distinct, registered class with their own obligations under Rule 4 and the First Schedule, from 13 November 2026.
- The **State and its instrumentalities** have their own legitimate uses (s.7(b)–(c)), standards (Rule 5; Second Schedule) and carve-outs (s.17(2)(a), s.17(4)).

Chapter 3 explains each role and the boundary of the Act's scope in detail.

1.4 Why it matters

The Schedule to the Act sets maximum penalties that are large by any standard: up to ₹250 crore for breach of the obligation to take reasonable security safeguards (Schedule item 1), up to ₹200 crore for failure to give the Board or affected Data Principals notice of a personal data breach (item 2) and for breach of the additional obligations relating to children (item 3), up to ₹150 crore for breach of the additional obligations of a Significant Data Fiduciary (item 4), and up to ₹50 crore for breach of any other provision of the Act or the

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-dpdpa · © 2026 Srida IT

REQUIREMENT TOPIC R-06 · S.6(7)–(9); RULE 4; FIRST SCHEDULE

Consent Managers

DPDP Act, 2023 / DPDP Rules, 2025 WP-R06

A Provisions and Summary

s.6(7)–(9); Rule 4; First Schedule — Consent Managers

A Data Principal may give, manage, review or withdraw consent to a Data Fiduciary through a Consent Manager — a company registered with the Board that operates an accessible, transparent and interoperable platform and is accountable to, and acts on behalf of, the Data Principal. Rule 4 and the First Schedule set the registration conditions (Part A: Indian company, capacity, net worth of at least two crore rupees, fit management, constitutional safeguards, independent certification) and the continuing obligations (Part B: direct and routed consent, data-blind sharing, seven-year records, website or app, no sub-contracting, security, fiduciary capacity, conflict-of-interest controls, ownership disclosures, audit and reporting, and no change of control without Board approval).

In force: From 13 November 2026 (three weeks after the date of this edition): s.6(9) (registration with the Board) and s.27(1)(d) (Board inquiry on intimation of breach of a registration condition) (G.S.R. 843(E) cl.(b)); Rule 4 and the First Schedule (Rule 1(3) as corrected by G.S.R. 892(E)). **From 13 May 2027:** s.6(7) (the Data Principal's right to act through a Consent Manager), s.6(8) (accountability to the Data Principal), s.27(1)(c) (complaints against Consent Managers), s.28 (Board procedure) and s.33 (penalties) (G.S.R. 843(E) cl.(c)). All dates carry the ±1 day qualification. Whether Part B obligations are enforceable, and whether penalties can be imposed, between 13 November 2026 and 13 May 2027 is open (REQ-CMG-06, below). In October 2026 nothing in this topic is yet in force.

Applies to: Two audiences. (1) Persons that act or propose to act as Consent Managers: only a company incorporated in India can meet First Schedule Part A item 1; Rule 4 and Part B apply from registration. (2) Data Fiduciaries whose Data Principals use, or who are onboarded onto, a registered Consent Manager platform. Data Fiduciaries do not register with the Board. A consent-management software product used by a fiduciary is not a Consent Manager unless its provider is registered and acts for the Data Principal (s.2(g)).

Summary in Srida IT's own words. The official Gazette text of the Act and Rules is authoritative.

B Statutory Requirements

Provision	Class	Requirement
s.6(7)	A — Legal requirement	The Data Principal may give, manage, review or withdraw her consent to the Data Fiduciary through a Consent Manager.
s.6(8); Rule 4(3); First Schedule Part B	A — Legal requirement	The Consent Manager is accountable to the Data Principal and acts on her behalf in the manner and subject to the obligations prescribed — the thirteen obligations in First Schedule Part B.
s.6(9); Rule 4(1)–(2); First Schedule Part A	A — Legal requirement	Every Consent Manager must be registered with the Board. A person meeting Part A may apply with the particulars, information and documents the Board publishes on its website; the Board may inquire and either register the applicant and publish its particulars on its website, or reject the application with reasons.
First Schedule Part A items 1–9	A — Legal requirement	Conditions: (1) company incorporated in India; (2) sufficient technical, operational and financial capacity; (3) sound financial condition and general character of management; (4) net worth not less than two crore rupees; (5) adequate business volume, capital structure and earning prospects; (6) directors, KMP and senior management of fairness and integrity; (7) MoA and AoA requiring adherence to Part B items 9–10, amendable only with Board approval; (8) operations in the interests of Data Principals; (9) independent certification of the interoperable platform against Board-published data protection standards and assurance framework, and of measures for Part B item 11.
First Schedule Part B items 1–5	A — Legal requirement	Enable consent to an onboarded fiduciary directly, or routed through another onboarded fiduciary that holds the data with consent (item 1 and Illustration); share data so that its contents are not readable by the Consent Manager (item 2); keep a record of consents given, denied or withdrawn, of notices and of sharing with transferee fiduciaries (item 3); give the Data Principal access to the record and, on request and per terms of service, a machine-readable copy, and keep it for at least seven years or longer as agreed or required by law (item 4); maintain a website or app, or both, as the primary means of access (item 5).

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-dpdpa · © 2026 Srida IT

Provision	Class	Requirement
First Schedule Part B items 6–10	A — Legal requirement	Do not sub-contract or assign the performance of any obligation under the Act and Rules (item 6); take reasonable security safeguards to prevent personal data breach (item 7); act in a fiduciary capacity in relation to the Data Principal (item 8); avoid conflicts of interest with Data Fiduciaries, including their promoters and KMP (item 9); have measures so that no conflict arises from directors, KMP or senior management holding directorships, financial interests, employment or beneficial ownership in, or material pecuniary relationships with, Data Fiduciaries (item 10).
First Schedule Part B items 11–13	A — Legal requirement	Publish on the website or app, easily accessibly, its promoters, directors, KMP and senior management; every holder of more than two per cent of its shares; every body corporate in which those persons hold more than two per cent as on the first day of the preceding calendar month; and other information the Board directs (item 11). Have effective audit mechanisms and report outcomes to the Board periodically and as directed, covering controls, continued fulfilment of registration conditions and adherence to obligations (item 12). Control must not be transferred by sale, merger or otherwise without the Board's previous approval and conditions (item 13).
Rule 4(4)–(6)	B — Regulatory power or guidance	The Board may, after a hearing, inform a non-adhering Consent Manager and direct measures (4(4)); may, in the interests of Data Principals and after a hearing, suspend or cancel registration and give protective directions by reasoned order (4(5)); and may require any information (4(6)).
s.27(1)(c)–(d)	B — Regulatory power or guidance	The Board may inquire into a Data Principal's complaint of breach by a Consent Manager of its obligations (from 13 May 2027) and into an intimation of breach of a registration condition (from 13 November 2026), and impose penalty as provided in the Act.

C Interpretation

A regulated intermediary, not a software category. The Act uses “Consent Manager” for a registered company acting for the Data Principal, not for the consent-management platforms that fiduciaries license to run cookie banners and preference centres. The two differ on every axis that matters: a Consent Manager is registered and listed by the Board, is accountable to the Data Principal, acts in a fiduciary capacity towards her, must avoid conflicts with Data Fiduciaries, must not be able to read the data shared and must not sub-contract its obligations. A fiduciary that describes its own tool as a “Consent Manager” in notices misdescribes it. Before relying on a Consent Manager, a fiduciary should confirm its registration on the Board's website and re-check it periodically, because registration can be suspended or cancelled (Rule 4(5)).

Uneven commencement. Registration (s.6(9)) and the Rule 4 regime start on 13 November 2026, but the right of the Data Principal to use a Consent Manager (s.6(7)) and the statutory accountability provision (s.6(8)) start only on 13 May 2027, as do complaint-based inquiries, Board procedure and penalties. During the first six months, Consent Managers can be registered and are bound by Rule 4(3) to Part B, and the Board can inquire into intimations of breach of registration conditions, but s.33 is not yet in force. The spine records the enforceability and penalty position in this window as unresolved (below). Applicants should nevertheless meet Part B from the day of registration.

Conditions that will need further Board publications. Rule 4(1) depends on the particulars the Board publishes for applications, and Part A item 9 depends on “data protection standards and assurance framework” the Board publishes; neither had been located when the spine was validated (17 September 2026), and the certification body for item 9 is not specified. Reporting periodicity and format under Part B item 12 await Board direction. Applicants can prepare evidence for each condition now, but cannot complete the application until the Board publishes. Part A item 7 requires constitutional documents to embed Part B items 9–10 (conflicts) and to be amendable only with the Board's previous approval, which means corporate approvals should be sought before applying.

Data-blind, routed consent. Part B item 1 and its illustration describe two flows: the Data Principal consents directly to an onboarded fiduciary, or routes consent through another onboarded fiduciary that already holds her data with consent and instructs it to send the data. Item 2 requires that the manner of sharing prevents the Consent Manager from reading the contents. The defensible architecture is one in which the Consent Manager handles consent artefacts and metadata while payloads are encrypted end-to-end between fiduciaries, with no decryption keys held by the Consent Manager. Records under item 3 cover consents, notices and sharing events; access, machine-readable export and a seven-year minimum retention follow under item 4. The boundary between prohibited sub-contracting (item 6) and ordinary use of hosting or IT service providers is marked for interpretive review in the spine; a defensible test is whether the vendor performs a Part B obligation or merely supplies infrastructure the Consent Manager uses to perform it.

The fiduciary's side. Whether a fiduciary that is not onboarded must accept consent or withdrawal routed through a registered Consent Manager is open (REQ-CMG-01). Where a fiduciary is onboarded, consent and withdrawal through the platform should have the same effect as direct consent, and the fiduciary still bears the burden of proving notice and consent under s.6(10); integration of the Consent Manager's consent artefacts into the fiduciary's own consent ledger is therefore advisable. Consent through a Consent Manager does not relieve the fiduciary of its s.5 notice duty, and Part B item 3(b) expects notices to precede or accompany requests on the platform.

SAMPLE

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-dpdpa · © 2026 Srida IT

D Open Legal Questions

Open legal question REQ-CMG-01 — legal counsel required

Must a Data Fiduciary accept consent, or a withdrawal of consent, that a Data Principal gives through a registered Consent Manager (s.6(7)), including where the fiduciary is not onboarded onto that platform?

Competing readings

- Reading 1: s.6(7) confers a right on the Data Principal; a right to act through a Consent Manager implies that fiduciaries must give effect to consent and withdrawal so communicated, at least for withdrawal, which s.6(4) requires to be comparably easy.
- Reading 2: s.6(7) is permissive ("may"), Part B item 1 operates only between onboarded fiduciaries, and nothing obliges a fiduciary to onboard; use of a Consent Manager is therefore optional for the fiduciary, though a withdrawal actually received must still be honoured under s.6(4)–(6). Srida IT's Legal Fact Sheet (§12) currently describes use as optional; the spine records that statement as unresolved.

Srida IT interim approach (practice, not law)

Srida IT practice: record a written position on Consent Manager use for the sector; whatever that position, honour any withdrawal that actually reaches the fiduciary through a registered Consent Manager as a withdrawal under s.6(4)–(6); if onboarded, ingest Consent Manager artefacts into the consent ledger; review the position when the Board publishes registrations or guidance. Legal counsel required.

Open legal question REQ-CMG-06 — legal counsel required

Are the First Schedule Part B obligations enforceable, and can a penalty be imposed on a Consent Manager, between 13 November 2026 (Rule 4, s.6(9), s.27(1)(d)) and 13 May 2027 (s.6(8), s.28, s.33)? Which Schedule entry applies to a Consent Manager's security failure under Part B item 7 (REQ-CMG-18)?

Competing readings

- Reading 1: Rule 4(3) and Part B bind registered Consent Managers from registration, and the Board's Rule 4(4)–(5) powers (directions, suspension, cancellation) operate from 13 November 2026; monetary penalties await s.33 on 13 May 2027.
- Reading 2: because s.6(8), which is the parent provision for Part B, and s.28 and s.33 commence only on 13 May 2027, Part B obligations are not enforceable through the Act's inquiry and penalty machinery until then, although registration conditions can be inquired into under s.27(1)(d).
- On the penalty entry: item 1 of the Schedule refers to the obligation "of Data Fiduciary" under s.8(5), so a Consent Manager's Part B item 7 failure may fall under item 7 (residual); a contrary view treats a Consent Manager that is also a fiduciary for its own processing as within item 1 for that processing.

Srida IT interim approach (practice, not law)

Srida IT practice: a Consent Manager complies with every Part B obligation from the date of registration and keeps evidence, regardless of the enforcement question; it treats Rule 4(4)–(5) directions as operative from 13 November 2026; and it obtains counsel's view on penalty exposure before relying on any gap. Legal counsel required.

E Implementation Guidance

1. **All fiduciaries:** record a position on whether the organisation will onboard onto any registered Consent Manager, considering sector practice and the REQ-CMG-01 question. Srida IT recommends reviewing the position when the Board publishes registrations.
2. **All fiduciaries:** verify registration on the Board's website before onboarding and at least quarterly; maintain a contingency runbook for suspension or cancellation that follows any Board directions protecting Data Principals.
3. **All fiduciaries:** design the consent ledger to ingest Consent Manager consent and withdrawal artefacts with their identifiers and audit trail, so that s.6(10) proof does not depend on the Consent Manager alone; ensure a withdrawal via the platform stops processing as a direct withdrawal would (R-05).
4. **All fiduciaries:** remove any description of an in-house or licensed consent tool as a "Consent Manager" from notices, contracts and marketing.
5. **Applicants:** build a Part A evidence matrix (incorporation, capacity, audited net worth of at least two crore rupees, business plan, fit-and-proper declarations, MoA/AoA clauses for Part B items 9–10, interests-of-Data-Principals assessment) and complete it against the Board's published particulars when available.
6. **Applicants:** engage an independent certifier with no implementation role for Part A item 9 once the Board publishes its standards and assurance framework; do not launch Consent Manager services until registration is published on the Board's website.
7. **Consent Managers:** implement the platform so that direct and routed consent (Part B item 1 cases) work, payloads are not readable by the Consent Manager (item 2, with documented key custody), and records of consents, notices and sharing are append-only, accessible to the Data Principal, exportable in machine-readable form and retained for at least seven years (items 3–4).
8. **Consent Managers:** map every Part B obligation to an internal owner; apply a procurement gate so that no vendor performs a Part B obligation (item 6); apply security safeguards equivalent to Rule 6 (item 7).

© 2026 Srida IT · Version 1.1 · Guidance, not legal advice · Refer to the official Gazette text

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-dpdpa · © 2026 Srida IT

9. **Consent Managers:** adopt a fiduciary-duty charter, annual and event-driven interest declarations, automated screening against onboarded fiduciaries, and recusal records (items 8–10); publish and refresh monthly the item 11 disclosures with a dated archive.
0. **Consent Managers:** operate an audit plan covering Part B item 12(a)–(c) at least annually until the Board specifies periodicity, a register of Board requests and directions (Rule 4(4), 4(6)), and a change-of-control gate making Board approval a condition precedent (item 13).

F Roles and Responsibilities

Role	Responsibility
Board of directors (Consent Manager)	Approves the fiduciary-duty charter, conflict-of-interest measures, MoA/AoA amendments and any change-of-control transaction subject to Board approval.
Compliance officer (Consent Manager)	Maintains the Part A condition matrix and Part B obligations matrix, monthly disclosures and the Board request register.
Platform / security lead (Consent Manager)	Implements data-blind sharing, record-keeping, availability of the website or app and security safeguards.
Independent certifier and auditor	Certifies the platform under Part A item 9 and audits Part B item 12 matters without implementation involvement.
Privacy lead (Data Fiduciary)	Owns the organisation's Consent Manager position, registration checks, ledger integration and contingency runbook.
Legal counsel	Advises on REQ-CMG-01, REQ-CMG-06, sub-contracting boundaries and change-of-control transactions.

G Documented Information and Records

Records required by the Act or Rules

- Consent Manager: record of consents given, denied or withdrawn, of notices preceding or accompanying requests, and of sharing with transferee fiduciaries, retained for at least seven years (First Schedule Part B items 3–4)
- Consent Manager: published disclosures of promoters, directors, KMP, senior management, holders of more than two per cent and related bodies corporate (Part B item 11)
- Consent Manager: audit outcomes reported to the Board periodically and as directed (Part B item 12)
- Consent Manager: MoA and AoA provisions required by Part A item 7
- Applicant: registration application with the particulars, information and documents the Board publishes (Rule 4(1))

Records recommended by Srida IT

- Data Fiduciary: Consent Manager position note, registration verification log and contingency runbook
- Data Fiduciary: consent-ledger integration specification for Consent Manager artefacts
- Consent Manager: Part A condition matrix with evidence and quarterly director-signed monitoring
- Consent Manager: Part B obligations matrix with owners and evidence links
- Consent Manager: key-custody architecture and independent test attempting payload access
- Consent Manager: conflict register, declarations and recusal records
- Consent Manager: outsourcing register classifying vendors against Part B item 6, with legal sign-off
- Consent Manager: Board request and direction register; change-of-control legal assessments

H Audit Testing Procedures

Recommended Srida IT audit methodology; not prescribed by the Act or the Rules.

Table 9-4. Audit testing procedures, Requirement R-06

Test ID	Method	Testing procedure	Result
TP-R06-01	INSPECT	**Data Fiduciary.** Inspect the list of Consent Managers the organisation is onboarded onto or receives artefacts from. For each, verify registration on the Board's published list on the test date and examine the log of periodic re-verification.	☐ In place ☐ In place w/ obs. ☐ Not in place ☐ N/A
TP-R06-02	RE-PERFORM	**Data Fiduciary.** Using a test identity, give and then withdraw consent through each Consent Manager the organisation is onboarded onto. Trace both events into the organisation's consent ledger and verify that the withdrawal stopped processing within the organisation's reasonable-time target.	☐ In place ☐ In place w/ obs. ☐ Not in place ☐ N/A
TP-R06-03	INSPECT	**Data Fiduciary.** Inspect notices, contracts and marketing material for any description of an unregistered tool or vendor as a “Consent Manager”, and examine the documented Consent Manager position and contingency runbook.	☐ In place ☐ In place w/ obs. ☐ Not in place ☐ N/A

SAMPLE

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-dpdpa · © 2026 Srida IT

Test ID	Method	Testing procedure	Result
TP-R06-04	**EXAMINE**	**Consent Manager.** Examine the Part A condition matrix and supporting evidence: certificate of incorporation, audited net worth of at least two crore rupees, capacity and business-plan evidence, fit-and-proper declarations, MoA/AoA clauses for Part B items 9–10 and the Board-approval amendment restriction, and the independent certification report. Verify the Board's registration intimation and website listing.	☐ In place ☐ In place w/ obs. ☐ Not in place ☐ N/A
TP-R06-05	**RE-PERFORM**	**Consent Manager.** Re-perform the two flows in Part B item 1 (direct consent; routed consent with instruction to the holding fiduciary) in a test environment and verify the records created for consent, notice and sharing events under item 3.	☐ In place ☐ In place w/ obs. ☐ Not in place ☐ N/A
TP-R06-06	**EXAMINE**	**Consent Manager.** Examine the key-custody architecture and the latest independent test attempting payload access by operators. Verify that no Consent Manager system or person holds keys capable of decrypting shared payloads (Part B item 2).	☐ In place ☐ In place w/ obs. ☐ Not in place ☐ N/A
TP-R06-07	**SAMPLE**	**Consent Manager.** Select a sample of Data Principal records (minimum 25, including records older than one year where available). Verify Data Principal access to each record, produce a machine-readable export, and confirm that retention locks prevent deletion before seven years (Part B item 4).	☐ In place ☐ In place w/ obs. ☐ Not in place ☐ N/A
TP-R06-08	**INSPECT**	**Consent Manager.** Inspect the published item 11 disclosure page and its dated archive for the last three months. Reconcile the disclosures with the register of members and with director, KMP and senior management declarations, including holdings of more than two per cent in other bodies corporate as on the first day of the preceding calendar month.	☐ In place ☐ In place w/ obs. ☐ Not in place ☐ N/A
TP-R06-09	**EXAMINE**	**Consent Manager.** Examine the conflict register, annual and event declarations, screening results against onboarded fiduciaries and recusal records (Part B items 9–10), and the outsourcing register with legal sign-off on whether any vendor performs a Part B obligation (item 6).	☐ In place ☐ In place w/ obs. ☐ Not in place ☐ N/A
TP-R06-10	**EXAMINE**	**Consent Manager.** Examine the audit plan and reports covering Part B item 12(a)–(c), evidence of submission to the Board, the register of Board requests and directions under Rule 4(4) and 4(6) with responses, and any change-of-control assessment showing Board approval as a condition precedent (item 13).	☐ In place ☐ In place w/ obs. ☐ Not in place ☐ N/A

I Interview Questions

Interviewee	Question
Privacy lead (Data Fiduciary)	Do you receive consents or withdrawals through any Consent Manager, and how did you confirm it is registered with the Board?
Privacy lead (Data Fiduciary)	If a customer withdraws consent through a Consent Manager, what happens in your systems, and how fast?
Compliance officer (Consent Manager)	Which Part A conditions depend on Board publications that have not yet appeared, and how are you tracking them?
Platform / security lead (Consent Manager)	Can anyone in your organisation read the personal data that flows between fiduciaries on your platform? How do you know?
Board of directors (Consent Manager)	How do you ensure platform and commercial decisions put Data Principals' interests first, and how are directors' interests in onboarded fiduciaries handled?
Legal counsel	What is your advice on obligations and penalty exposure between 13 November 2026 and 13 May 2027?

J Expected Audit Evidence

- Board website listing of registered Consent Managers and the organisation's verification log
- Consent ledger entries for Consent-Manager-sourced consents and withdrawals
- Consent Manager position note and contingency runbook
- Part A condition matrix, incorporation and net-worth evidence, MoA/AoA extracts, independent certification report
- Test results for direct and routed consent flows
- Key-custody documentation and independent payload-access test report
- Record samples, machine-readable exports and retention-lock configuration
- Dated archive of item 11 disclosures and reconciliation
- Conflict register, declarations, outsourcing register
- Audit reports, Board submissions and Board request/direction register

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-dpdpa · © 2026 Srida IT