

Consent Managers Under the DPDP Act: What Businesses, Investors and Applicants Must Know Before Registration Begins

India's Digital Personal Data Protection Act, 2023 ("DPDP Act"), together with the notified Digital Personal Data Protection Rules, 2025 ("DPDP Rules"), creates a regulated category of intermediary known as the **Consent Manager**. Its purpose is to make consent easier for individuals to give, manage, review and withdraw across participating businesses.

The concept offers an important commercial opportunity, but it is not simply a new label for privacy software. A statutory Consent Manager must obtain registration from the Data Protection Board of India ("Board"), meet demanding eligibility criteria and operate as an independent, accountable intermediary acting in the interests of individuals.

For technology entrepreneurs, existing businesses, investors and professional advisers, the immediate questions are practical: who may register, how much capital is needed, what infrastructure must be developed, what activities are prohibited and when do the obligations take effect?

What exactly is a Consent Manager?

Section 2(g) of the DPDP Act defines a Consent Manager as a person registered with the Board who acts as a single point of contact to enable a Data Principal to give, manage, review and withdraw consent through an accessible, transparent and interoperable platform.

The **Data Principal** is the individual to whom the personal data relates. The **Data Fiduciary** is the person who determines the purpose and means of its processing. A Consent Manager

sits between these participants for consent-related interactions, but does not take over the Data Fiduciary's statutory responsibilities.

For instance, where a customer authorises a bank to obtain an account statement held by another onboarded bank, the Consent Manager can convey and record that authorisation. The underlying statement must be shared in a manner that does not make its contents readable by the Consent Manager.

Is every business required to appoint a Consent Manager?

No. The Act permits an individual to give, manage, review or withdraw consent through a registered Consent Manager, but does not make this channel compulsory for all businesses or all individuals. A Data Fiduciary can administer consent through its own legally compliant systems.

There is also a critical distinction between a registered Consent Manager and a **consent-management platform** supplied to a particular company. A software vendor does not automatically become a statutory Consent Manager merely because its product maintains consent logs or displays privacy banners.

When does the registration regime begin?

The Central Government notified phased commencement of the Act and final Rules in November 2025. The principal stages, calculated from publication of the Gazette on 13 November 2025, are:

13 November 2025: Specified preliminary, institutional and procedural provisions, including the framework establishing the Board, came into force.

13 November 2026: Section 6(9), Section 27(1)(d) and Rule 4 governing Consent

Manager registration and supervision are scheduled to commence.

13 May 2027: The principal obligations relating to consent, notices, security, individual rights, grievances and the broader penalty regime are scheduled to commence.

The later two dates are calculated from the notification's one-year and eighteen-month periods. Applicants should verify any subsequent official clarification, technical standards or Board directions before applying.

Who can become a registered Consent Manager?

Rule 4 read with **Part A of the First Schedule** sets out nine cumulative conditions. The applicant must:

- **1. Be incorporated in India:** Registration is available to an Indian company, not directly to a sole proprietor, ordinary partnership or unincorporated undertaking.
- **2. Demonstrate sufficient capacity:** Technical, operational and financial resources must be adequate to perform its statutory functions.
- **3. Have sound finances and management:** The applicant's financial condition and general character of management must be satisfactory.
- **4. Maintain minimum net worth of Rs. 2 crore:** Net worth means total assets minus liabilities as appearing in the company's books of account. It is not merely a minimum paid-up capital requirement.
- **5. Have an adequate business plan:** Expected business volume, capital structure and earning prospects must be credible.
- **6. Establish integrity of leadership:** Directors, key managerial personnel and senior management must have a general reputation and record of fairness and integrity.
- **7. Amend its constitutional documents:** The memorandum and articles must secure

compliance with the prescribed conflict-of-interest requirements, with specified amendments subject to prior Board approval.

- **8. Act in the interests of individuals:** Proposed operations must be in the interests of Data Principals.
- **9. Obtain independent certification:** The interoperable platform and relevant technical and organisational measures must satisfy the standards and assurance framework published by the Board.

The minimum net-worth threshold should not be mistaken for the entire establishment cost. Certification, cybersecurity, technology development, skilled personnel, audit and operational resilience can require significant additional expenditure.

How will registration be granted?

A qualifying applicant may apply to the Board with the particulars, information and documents published on the Board's website. The Board may conduct inquiries to verify compliance with Part A. If satisfied, it must register the applicant and publish its particulars; otherwise, it must communicate the reasons for rejection.

The Rules do not, by themselves, fix a universal application fee, a guaranteed processing period or a detailed technical application template. These operational details must be checked against subsequent official publications. **Developing a platform or submitting an application does not itself confer registered status.**

What must a Consent Manager actually do?

Part B of the First Schedule prescribes thirteen continuing obligations. They should shape the business model from the outset, rather than being treated as post-registration formalities.

1. Facilitate consent across onboarded businesses

The platform must enable a Data Principal to give consent directly to an onboarded Data Fiduciary or through another onboarded Data Fiduciary holding the relevant personal data with that individual's consent. Effective integration with participating organisations is therefore essential.

2. Ensure that personal data is not readable by it

The manner of making data available or sharing it must ensure that the **underlying contents are not readable by the Consent Manager**. This calls for a genuinely data-blind architecture, supported by suitable encryption, access restrictions and secure data-sharing design.

However, consent histories, identities and transaction metadata may themselves constitute personal data. They cannot be treated as unregulated simply because the underlying bank statement, health record or other file is not readable.

3. Record grants, refusals, withdrawals and sharing

The platform must maintain records of consents **given, denied or withdrawn**, the notices preceding or accompanying consent requests, and sharing of personal data with transferee Data Fiduciaries. Reliable timestamps, transaction identifiers and tamper-evident audit trails are sensible implementation measures.

4. Give access and preserve records for seven years

Individuals must be able to access the prescribed records and, on request in accordance with the terms of service, receive the information in a machine-readable form. The records must be maintained for **at least seven years**, or longer where the parties agree or the law requires. This is a rule concerning consent-related records; it should not be read as permission to retain every category of underlying personal data indefinitely.

5. Maintain a website or application

A website, mobile application or both must be the primary channel through which Data Principals access the service. Accessibility, clarity, multilingual usability and uncomplicated withdrawal journeys should be treated as design priorities.

6. Do not subcontract statutory obligations

The Rules expressly prohibit a Consent Manager from subcontracting or assigning performance of its obligations under the Act and Rules. This is a particularly important restriction for start-ups intending to outsource their entire regulated operating model.

The Rules do not comprehensively explain the boundary between prohibited delegation of obligations and purchasing ancillary services such as cloud hosting or security tooling. Contracts should therefore preserve the Consent Manager's direct control and accountability, pending further regulatory clarification.

7. Maintain reasonable security safeguards

The platform must take reasonable security safeguards to prevent personal data breaches. Access controls, encryption, monitoring, vulnerability assessment, incident management, secure backups and business-continuity arrangements are central components of an effective security programme.

8. Act in a fiduciary capacity

The Consent Manager must act in a **fiduciary capacity in relation to the Data Principal**. Commercial considerations must not improperly influence the individual's ability to make a free choice. A platform designed to pressure users into approval, frustrate withdrawals or unfairly favour selected businesses would create serious regulatory concerns.

9 and 10. Avoid conflicts of interest

The Consent Manager must avoid conflicts with Data Fiduciaries, including conflicts involving their promoters and key managerial personnel. It must establish safeguards against conflicts caused by its own directors, key managerial personnel or senior management holding directorships, financial interests, employment, beneficial ownership or material pecuniary relationships with Data Fiduciaries.

This may affect ownership structures, investor participation, related-party arrangements and collaborations with large technology or financial institutions. Conflict checks should be undertaken before incorporation or fundraising, not merely at the time of registration.

11. Make prescribed ownership disclosures

The website or application must disclose promoters, directors, key managerial personnel and senior management; persons holding more than **2% of the Consent Manager's shares**; prescribed corporate shareholdings of leadership persons above 2%; and additional details that the Board may direct. Maintaining a current disclosure register will be essential.

12. Establish effective audits

The Consent Manager must maintain mechanisms to review, monitor and evaluate technical controls, continuing eligibility and compliance with the Act and Rules, and report audit outcomes to the Board periodically or as directed. The precise reporting cadence should be taken from applicable regulatory directions; the First Schedule does not itself prescribe one universal annual cycle.

13. Obtain approval before a change of control

Control of a registered Consent Manager cannot be transferred through sale, merger or otherwise without the Board's previous approval. Share acquisitions, group restructuring and investor exits must be assessed for this restriction and appropriate regulatory conditions precedent.

How should the platform work in practice?

A typical workflow begins with secure onboarding and authentication of the individual, followed by integration of participating Data Fiduciaries. The individual receives a purpose-specific consent request with the relevant notice, makes an affirmative decision and receives an accessible record. Later, the individual can review the history or withdraw the consent through the same interface.

The Consent Manager must communicate the decision reliably. However, the **Data Fiduciary** remains responsible for providing a lawful notice, establishing a valid basis for processing, honouring withdrawal and complying with other applicable duties. Consent management is not a device for transferring away the Data Fiduciary's legal liability.

Consent must be free, specific, informed, unconditional and unambiguous, expressed through clear affirmative action. Withdrawal must be as easy as granting consent. These substantive requirements form part of the later operational phase under Section 6.

What should different stakeholders examine?

Individuals: Can they understand who seeks consent, for what purpose and for which information? Can they decline or withdraw without manipulative design? Can they access the historical record?

Data Fiduciaries: Do the platform's notices and consent events correspond with actual processing? Are withdrawals implemented across processors? Are records sufficient to support the Data Fiduciary's statutory burden of proof?

Technology providers: Are they merely selling enterprise consent tools, or seeking to

undertake the separately regulated Consent Manager role? Do contracts and outsourced arrangements comply with the non-subcontracting restriction?

Investors and acquirers: Will shareholding, related-party interests, board appointments or control rights create conflicts? Does the applicant have sufficient sustainable capital, independent certification and a credible governance structure?

Banks, insurers, hospitals and telecom operators: Can existing sectoral compliance obligations operate alongside the new consent architecture? Sector-specific approvals are not substitutes for DPDP Consent Manager registration.

Can a bank or Account Aggregator become a Consent Manager?

A banking, financial-technology or Account Aggregator business should not assume that an existing sectoral authorisation automatically satisfies DPDP registration. The RBI Account Aggregator regime and the DPDP Consent Manager regime have different legal sources and requirements.

An applicant associated with Data Fiduciaries must also assess whether its corporate structure or relationships can comply with the statutory independence and conflict rules. Eligibility therefore requires a case-specific evaluation rather than a general assumption of permission or prohibition.

What business model is commercially sustainable?

Potential revenue arrangements may involve neutral platform-access charges, onboarding or integration fees, technology support and other transparent service charges. The Rules do not prescribe a single mandatory tariff or business model.

Nevertheless, a business model that rewards higher consent-approval rates, discourages

withdrawal or makes the platform dependent upon preferential treatment of a particular Data Fiduciary may undermine the fiduciary and conflict-of-interest requirements. **Commercial neutrality is likely to be a decisive long-term trust factor.**

What are the risks, penalties and remedies?

Under Rule 4, following the prescribed opportunity of hearing, the Board may direct corrective measures for non-compliance. Where necessary in the interests of Data Principals, it may suspend or cancel registration, record reasons and issue protective directions. Loss of registration may be commercially more serious than an ordinary compliance notice.

The Act separately provides for inquiries concerning registration-condition breaches and, when the relevant later provisions commence, complaints about Consent Manager obligations. Section 33 and the Schedule provide for monetary penalties, with the residual category for breach of other provisions of the Act or Rules capped at **Rs. 50 crore**. The actual statutory ground, significance of breach, commencement status and procedure must be examined in each case; the maximum is not an automatic penalty.

Individuals have a statutory grievance-redressal framework, with Rule 14 requiring a published period not exceeding ninety days once operative. Appeals against appropriate Board orders lie before the Appellate Tribunal under Section 29, subject to the statutory limitation and procedure. The designated appellate forum is TDSAT.

What should an aspiring applicant do now?

A practical readiness programme should ordinarily include the following steps:

- **Corporate due diligence:** Confirm Indian incorporation, financial records, net worth, shareholding, management suitability and constitutional-document amendments.
- **Conflict mapping:** Identify direct and indirect interests of promoters, directors, management and investors in Data Fiduciaries; establish preventive controls and disclosure processes.
- **Business planning:** Prepare realistic projections for development, operating expenditure, audits, certification and sustained availability of the service.
- **Technology architecture:** Build a secure interoperable platform capable of consent grants, refusals, review, withdrawal, notice capture, machine-readable exports and data-blind sharing.
- **Documented governance:** Prepare terms of service, security and incident-response policies, record-retention practices, grievance processes, internal audit programmes and regulatory reporting controls.
- **Certification readiness:** Monitor and meet the Board's published data-protection standards, assurance framework and independent certification requirements.
- **Regulatory filing:** Submit the documents actually prescribed on the Board's website; respond to inquiries and obtain formal registration before representing the entity as a statutory Consent Manager.
- **Continuing compliance:** Monitor audits, disclosures, security, conflicts, ownership changes, record retention and directions of the Board throughout the life of the business.

What remains to be clarified?

Important practical questions include the technical standards for interoperability, qualifying independent certification arrangements, the permissible extent of ancillary outsourcing, the treatment of sector-regulated entities, the fee and documentary application process, and the scope of acceptable commercial relationships with Data Fiduciaries.

Applicants should distinguish clearly between **express legal requirements** and **recommended technical practices**. Encryption architecture, API standards, certification bodies and additional application documents should not be described as finally mandated unless supported by the applicable official publications.

The time to prepare is now

The Consent Manager regime creates an opportunity to build independent digital trust infrastructure in India. But the regulatory gateway is unusually demanding for an emerging technology business: Indian incorporation, Rs. 2 crore net worth, fit-and-proper management, independent technical certification, data-blind operations, seven-year records, fiduciary accountability and strict conflict controls.

Businesses seeking registration should begin with a **corporate, technical and regulatory gap assessment** and build their operating model around Data Principal interests. For stakeholders integrating such platforms, the priority is to preserve the distinction between consent facilitation and the Data Fiduciary's continuing legal responsibility.

The ultimate measure of success will be whether Consent Managers make digital consent a genuine exercise of individual choice rather than another formal compliance checkbox.

Statutory references

Digital Personal Data Protection Act, 2023: Sections 2(g), 5, 6, 13, 27, 29 and 33, and the Schedule. Digital Personal Data Protection Rules, 2025: Rules 1, 4 and 14, and Parts A and B of the First Schedule. Commencement Notification G.S.R. 843(E), dated 13 November 2025; Rules Notification G.S.R. 846(E), dated 13 November 2025; Corrigendum G.S.R. 892(E), dated 10 December 2025. Official texts: www.meity.gov.in.

This article is intended solely for general information and awareness and does not constitute solicitation or legal advice for any specific factual situation. The regulatory position should be rechecked against subsequent notifications and directions.

Contact us at:-

Mr. Himanshu Dhawan, Advocate
Mr. Shubham Jain,
Advocate-on-Record, Supreme Court
of India

Contact@utkrishthalaw.com

Ph - +91-9999309222;
+91-8750021607

www.utkrishthalaw.com