Consent Manager under the DPDP Act: A New Institutional Layer for India's Data Protection Regime

INTRODUCTION

The Digital Personal Data Protection Act, 2023 (**DPDP Act**), read with the Digital Personal Data Protection Rules, 2025 (**DPDP Rules**), places ***'consent'*** at the centre of India's data protection regime. In most contexts (unless exempted by law), consent is the sole legal basis for processing digital personal data.

The DPDP Act sets a high bar for consent - it must be free, specific, informed, unconditional, and unambiguous; preceded by an itemised notice; obtained separately for each processing purpose; and as easy to withdraw as it was to give. However, when individuals are required to repeatedly provide consent across dozens of daily digital interactions, the process often becomes mechanical rather than informed or meaningful. This phenomenon, widely recognised as "*consent fatigue*," is a well-documented challenge in data protection frameworks globally. The DPDP Act's response to this problem is the 'Consent Manager' framework, a registered intermediary that acts as a single point of contact, enabling data principals to give, manage, review, and withdraw consent across data fiduciaries through an accessible, transparent, and interoperable platform.

This primer examines the Consent Manager framework under the DPDP Act and DPDP Rules, its statutory foundations, key obligations, and the practical considerations businesses will need to navigate as the framework becomes operational.

THE CONSENT MANAGER ARCHITECTURE: KEY PROVISIONS

- ***What operational challenge does the Consent Manager framework seek to address?***

The cumulative effect is a framework that expects every data principal to maintain an active, granular consent relationship with every data fiduciary processing her data. For an individual using even a handful of digital services daily, this translates into dozens of overlapping consent relationships, each with its own notice, purpose, and withdrawal mechanism.

The Consent Manager is the DPDP Act's institutional response to this problem. It is a registered intermediary that serves as a single point of contact, enabling data principals to give, manage, review, and withdraw consent across multiple data fiduciaries from one accessible platform, rather than navigating each platform's privacy settings independently.

FOR EXAMPLE

A data principal who has consented to processing by an e-commerce platform, a health-tech app, and a financial services provider would ordinarily need to locate each platform's privacy settings separately to modify or withdraw consent.

Through a Consent Manager, she could view all active consents in a single dashboard and act on them with comparable ease across providers.

It is also important to note that, Consent Managers are intended to operate as "data blind" intermediaries, meaning they facilitate and manage consent without accessing the underlying personal data.

- ***Provisions under the DPDP Act***

Section 6(7) establishes the Consent Manager as an intermediary channel through which a data principal may give, manage, review, or withdraw consent to the data fiduciary. **Section 6(8)** adds a fiduciary-like duty: the consent manager must be accountable to the data principal and act on her behalf, not a routine vendor relationship, but a statutory obligation that places the data principal's interest at the centre. **Section 6(9)** requires registration with the Data Protection Board of India (**DPBI**) and compliance with prescribed technical, operational, and financial conditions.

Accountability does not end there. **Section 13** requires Consent Managers to maintain readily available grievance redressal mechanisms and resolve complaints within prescribed timelines. Lastly, **Section 27** empowers the DPBI to inquire into complaints against Consent Managers and to impose penalties for breach of obligations or registration conditions.

THE CONSENT MANAGER FACES ENFORCEMENT EXPOSURE FROM TWO DIRECTIONS

From data principals through grievance redressal under Section 13, and from the DPBI through inquiry and penalty powers under Section 27. Unlike a data processor, which is typically shielded behind its contract with the data fiduciary, the Consent Manager has no such buffer and is directly and independently liable under the statute.

- ***Provisions under the DPDP Rules***

Rule 4 sets out the registration lifecycle for Consent Managers. Only entities meeting the First Schedule eligibility conditions, including incorporation in India and a minimum net worth of two crore rupees, may apply. Registration is subject to ongoing oversight, with the DPBI empowered to monitor compliance, require corrective action, and suspend or cancel registration where necessary in the interest of data principals.

Rule 14 requires both data fiduciaries and Consent Managers to prominently publish relevant details of how data principals may exercise their rights and to establish grievance redressal systems within ninety days. It also permits data principals to nominate individuals to exercise their rights on their behalf, which may be relevant in contexts involving minors or dependents.

- ***Registration Criterions and Obligations***

If a business intends to establish a Consent Manager platform, the First Schedule prescribes nine conditions that an applicant must satisfy before the DPBI may grant registration. These can be broadly grouped as follows:

CATEGORY	CONDITION
Corporate structure	Must be a company incorporated in India. Memorandum and articles of association must embed Consent Manager obligations and require DPBI approval for amendments to those provisions.
Financial standing	Minimum net worth of INR 2 crore. Capital structure, earning prospects, and likely volume of business must be adequate. Financial condition and general character of management must be sound.

Management quality	Directors, key managerial personnel, and senior management must have a general reputation and record of fairness and integrity.
Technical readiness	Must have sufficient technical, operational, and financial capacity. Must obtain independent certification that its interoperable platform meets data protection standards published by the DPBI and that appropriate technical and organisational measures are in place.
Data principal interest	Proposed operations must be in the interests of data principals.

Once registered, a Consent Manager is subject to thirteen ongoing obligations under the First Schedule, spanning the full range of its operations. From a business perspective, these are the key thresholds and constraints that need to be carefully evaluated before onboarding a Consent Manager:

CATEGORY	OBLIGATION
Core consent functions	Enable data principals to give, manage, review, and withdraw consent to processing by onboarded data fiduciaries, either directly or routed through another onboarded fiduciary. Ensure that personal data shared through the platform is not readable by the Consent Manager itself.
Record-keeping	Maintain records of all consents given, denied, or withdrawn; all notices accompanying consent requests; and all instances of data sharing with transferee data fiduciaries. Provide data principals access to these records, including in machine-readable form on request. Retain records for a minimum of seven years.
Platform requirements	Develop and maintain a website or app (or both) as the primary channel for data principal access. Must not sub-contract or assign performance of any obligations.
Fiduciary duty & conflicts	Act in a fiduciary capacity in relation to the data principal. Avoid conflict of interest with data fiduciaries, including at the promoter and Key Managerial Personnel (**KMP**) level. Maintain measures to prevent conflicts arising from directors, KMP, or senior management holding directorships, financial interests, employment, or beneficial ownership in data fiduciaries.
Transparency & disclosure	Publish details of promoters, directors, KMP, senior management, and all shareholders holding above 2% of the Consent Manager's shareholding. Disclose body corporates in which any promoter, director, KMP, or senior management holds above 2% shareholding. Comply with any additional disclosure directions from the DPBI.
Security & audit	Take reasonable security safeguards to prevent personal data breach. Maintain effective audit mechanisms covering technical controls, continued fulfilment of registration conditions, and adherence to statutory obligations with periodic reporting to the DPBI.
Change of control	Control of the registered Consent Manager cannot be transferred by sale, merger, or otherwise without prior DPBI approval and fulfilment of DPBI-specified conditions.

KEY CONSIDERATIONS FOR BUSINESSES

- ***Registration is not compulsory for all consent management activity.*** Registration is not mandatory for all consent management activity. The DPDP Act defines a "Consent Manager" as a person registered with the DPBI, and ordinary enterprise consent management platforms **(CMPs)** used by data fiduciaries to manage cookies, preferences, or withdrawal requests would generally fall outside this definition since they act on behalf of the data fiduciary, not the data principal. However, where a CMP begins functioning as an independent, cross-platform consent intermediary for individuals, the line may blur and registration may need to be considered. Businesses should also note that adopting a Consent Manager framework is itself optional under the DPDP Act. Data fiduciaries may continue to manage consent directly through their own CMPs and internal systems, so long as they remain compliant with the Act's consent and rights-management requirements.
- ***Consent managers and enterprise CMPs must ideally co-exist.*** Data fiduciaries will continue using internal CMPs for compliance workflows. Simultaneously, data principals may route consent actions through registered Consent Managers. These two systems will need to talk to each other. Businesses should build APIs or data exchange protocols that allow registered Consent Managers to communicate consent actions, including withdrawal, in real time. Friction or delay in this relay is a regulatory risk.
- ***The Consent Manager is not your processor.*** A registered Consent Manager carries independent statutory obligations and a fiduciary duty to the data principal. It cannot be treated as a vendor operating at the data fiduciary's instructions. Businesses must account for this distinction in their contractual and operational arrangements.
- ***Consent fatigue is relocated, not resolved, unless the design is simplified.*** If Consent Managers simply replicate the notice-and-consent experience in a centralised interface, it does not solve the problem they were created to solve in the first place. For the framework to deliver on its promise, Consent Managers will need to invest in plain-language summaries, intuitive interfaces, and granular, purpose-specific controls and businesses should factor this into their selection criteria.
- ***Conflict-of-interest requirements will significantly shape who can operate as a Consent Manager.*** The First Schedule restricts directors, KMP, and senior management of a Consent Manager from holding directorships, financial interests, or beneficial ownership in data fiduciaries. For businesses that are data fiduciaries, or part of a wider group that includes them, this creates a structural constraint on setting up or investing in a Consent Manager. Companies should therefore assess group-level affiliations early, as even indirect shareholding above prescribed thresholds could affect eligibility or lead to post-registration non-compliance.

Lastly, businesses building consent management systems should prioritise simplicity, plain-language interfaces, and genuine user control over checkbox compliance. Equally, businesses selecting a Consent Manager should evaluate whether the platform meaningfully reduces consent fatigue for their users, not merely whether it satisfies the registration requirements under the Act.

We hope you have found this information useful. For any queries/clarifications please write to us at insights@elp-in.com or write to our authors:

Ravisekhar Nair, Partner – Email -*ravisekharnair@elp-in.com*

Sanjana S, Associate – Email – *sanjanas@elp-in.com*