ADVOCATES & SOLICITORS

CONSENT MANAGERS IN INDIA

THE NEXT BIG OPPORTUNITY IN DATA GOVERNANCE

Understanding data consent architecture, regulatory obligations, interoperability standards, audit readiness, and governance expectations

2025

Prepared by:

AK & Partners

About the Founders

Anuroop Omkar
Managing Partner

Anuroop is known for his strategic counsel to foreign investors, financial institutions, and fintech companies in India. With a decade of cross-border advisory experience, he has led mandates across banking regulation, digital lending, and insolvency turnaround. His blend of legal insight and commercial foresight makes him a trusted advisor. Anuroop is also a noted speaker and author on fintech policy and RBI regulations. He is committed to delivering fast, viable, and regulatorily sound solutions.

Kritika Krishnamurthy
Managing Partner

Kritika specialises in business advisory, from developing the most efficient strategy to expanding the business with growth capital, along with managing all material risks that come in the way. She advises banks, fintechs, and global investors on regulatory strategy, negotiations, enforcement, and cross-border transactions, with expertise in digital lending, PPI, and financial regulation. A published author and speaker on fintech governance, she is known for her fast, solution-driven, and business-aligned approach.

Awards & Recognitions

Chambers RANKED IN FinTech 2025 Leading Firm

The LEGAL 500 ASIA PACIFIC TOP TIER LIST 2023

The LEGAL 500 ASIA PACIFIC LEADING FIRM 2024

The LEGAL 500 ASIA PACIFIC INDIA CITY FOCUS 2023

The LEGAL 500 ASIA PACIFIC INDIA CITY FOCUS 2024

IFLR1000 RECOMMENDED FIRM 2024

BW LEGAL WORLD 40 UNDER 40

Forbes Presents LEGAL POWERLIST 2020 in association with legitquest BANKING & FINANCE ENLISTED AS THE TOP LAW FIRM

Forbes Presents LEGAL POWERLIST 2021 in association with legitquest BANKING & FINANCE ENLISTED AS THE TOP LAW FIRM

Forbes Presents LEGAL POWERLIST 2022 in association with legitquest BANKING & FINANCE ENLISTED AS THE TOP LAW FIRM

Forbes Presents LEGAL POWERLIST 2023 in association with legitquest BANKING & FINANCE ENLISTED AS THE TOP LAW FIRM

ALB INDIA FIRMS TO WATCH 2023 THOMSON REUTERS

RECOGNIZING EXCELLENCE IN CLIENT SERVICE CLIENT CHOICE

INDIA BUSINESS LAW JOURNAL AWARD WINNING LAW FIRM 2024 LAW ASIA

INDIA BUSINESS LAW JOURNAL FUTURE LEGAL LEADERS 2020 LAW ASIA

INDIA BUSINESS LAW JOURNAL AWARD WINNING LAW FIRM 2024 LAW ASIA

RECOGNIZING EXCELLENCE IN CLIENT SERVICE CLIENT CHOICE

Forbes INDIA LEGAL POWERLIST 2021 Top Law Firm in Banking & Finance

The LEGAL 500 FIRMS TO WATCH

ASSOCHAM INDIA

Executive Summary

The Digital Personal Data Protection ("**DPDP**") Act, 2023 of India establishes a comprehensive framework empowering individuals with control over their personal data and introducing Consent Managers as pivotal entities to facilitate seamless, secure, and user-centric consent lifecycle management. Consent Managers act as neutral intermediaries that enable individuals to grant, review, and withdraw consent across sectors including fintech, insurance, healthcare, retail, telecom, and government services. Through interoperable platforms and rigorous security protocols, these entities ensure that data sharing is subject to explicit, granular, and revocable consent, enhancing both privacy and convenience while promoting compliance with the Act's stringent obligations.

Consent Managers drive innovation in data portability, exemplified through use cases like NBFC, Fintech loan assessments, insurance policy portability, healthcare data sharing under the Ayushman Bharat Digital Mission, unified consumer consent dashboards, and government service validations. They provide crucial audit trails, grievance mechanisms, and transparency reporting, holding themselves and Data Fiduciaries accountable. The framework mandates robust management standards, financial threshold. This regulatory design aims to foster a trusted, efficient, and privacy-respecting digital ecosystem benefiting businesses and individuals alike.

Table of Contents

Guide to Consent Managers in India under DPDP Act

The DPDP Act, 2023, has introduced a new class of Regulated Entity - (CONSENT MANAGER), to strengthen user control over personal data.

Consent Manager - "*a person r***egistered with the Data Protection Board** *who acts as a single point of contact to enable Data Principal to give, manage, review and withdraw her consent through an accessible, transparent and interoperable platform*".

Consent must be specific, free, informed, unconditional, unambiguous, and given by clear affirmative action.	Consent Managers provide benefits to both Data Principals (efficient control of consent) and Data Fiduciaries (compliance facilitation).
Must implement robust data security safeguards such as encryption and maintain records of consents and data sharing actions for at least seven years.	Required to publish transparency information on promoters, directors, key managerial personnel, and shareholders with significant equity.
Prohibited from subcontracting or transferring control without prior approval from the Data Protection Board.	Authorized to audit and ensure compliance with DPDP Act obligations, and subject to suspension or cancellation by the Board for non-compliance.

Facilitates faster and secure personal data exchange in sectors like healthcare and finance by ensuring lawful consent-based data transfers.	Consent Managers' platform should ensure they cannot access readable personal data themselves, preserving privacy and security.

The role is expected to gain importance as a tech-enabled service under the new Indian data protection regime.

Scope

Provide a unified, centralized platform for Data Principals to manage consent across multiple services and sectors.

Convenience: Eliminates need to give or revoke consent separately on each website or app.

Accessibility: Platform must be user-friendly and transparent to diverse users.

Interoperability: Must follow common technical standards enabling seamless integration by any Data Fiduciary.

Consent Lifecycle: Covers entire process – initial consent, periodic reviews, and withdrawal.

Optional Use: Using a Consent Manager is voluntary for Data Principals but highly empowering.

Legal Validity: Consents or withdrawals made via a registered Consent Manager are legally valid and must be recognized by Data Fiduciaries.

Aggregated Choice: Provides a central dashboard for consent management without replacing direct consent on service platforms.

Transparency & Control: Enhances Data Principal's control over personal data sharing and privacy.

Supporting Data Rights: Facilitates grievance redressal, rights exercise, and complaint lodging through accessible tools.

Compliance Enhancement: Simplifies statutory consent obligations for Data Fiduciaries.

Support for DPDP Rules: Assists implementation of mandated privacy notices requiring easy consent withdrawal and rights exercise mechanisms.

Registration Conditions & Eligibility Criteria

Who can become a Consent Manager

- Applicant must be a company incorporated in India; individuals or foreign entities cannot register directly
- Minimum net worth of ₹2 Crore, demonstrated via audited financial documents and maintained on an ongoing basis.
- Must possess the necessary technology infrastructure, skilled personnel, and financial resources to run a secure, consent management platform.
- Directors, Key Managerial Personnel (KMP), and senior management must be persons of integrity, with no history of fraud, dishonesty, or serious regulatory violations.
- The applicant should have a credible plan and sustainable financial model for offering consent management services, ensuring long-term operational viability.
- The company's MoA and AoA must embed provisions preventing conflicts of interest, particularly avoiding alignment with Data Fiduciaries or related parties; amendments require prior Board approval.
- The business model and operations must align with empowering users and protecting their data rights, not exploiting consents for profit.

The technology platform must receive an independent certification confirming interoperability with Board-published standards and adherence to technical and organizational compliance obligations

Registration Process

Application to the Data Protection Board accompanied by necessary documents; the Board conducts scrutiny and inquiries before granting registration.

Meeting net worth, governance, conflict-of-interest, and operational criteria is an ongoing requirement; the Board may request information, impose conditions, or suspend/cancel registrations upon non-compliance.

Consent Managers must publish detailed information about promoters, directors, KMP, senior management, significant shareholders, and related corporate entities on accessible platforms.

Consent Managers must publish detailed information about promoters, directors, KMP, senior management, significant shareholders, and related corporate entities on accessible platforms.

Core Responsibilities of a Consent Manager

1

Enabling and Managing Entire Consent Lifecycle

- Facilitate giving, reviewing, and withdrawing consent for multiple Data Fiduciaries.
- Provide user interfaces for clear, simple consent actions.
- Support routing of consent across Data Fiduciaries as needed

2

Ensuring Data Security and Privacy

- Guarantee that personal data transmitted or shared is not readable or accessible by the Consent Manager.
- Use encryption and secure protocols to protect data in transit and at rest.
- Maintain tamper-proof records of all consent events, data sharing, and notices

3

Maintain Transparency, Accountability, and Compliance

- Keep detailed records of all consent activities for at least 7 years.
- Act as a fiduciary, prioritising Data Principal's interests and rights.
- Maintain tamper-proof records of all consent events, data sharing, and notices
- Ensure platform accessibility, easy user interface, and regular audits.
- Avoid conflicts of interest with Data Fiduciaries.
- Disclose ownership, governance, and operational details publicly.
- Conduct periodic audits and submit compliance reports to the Board.
- Prevent transfer or outsourcing of core functions without prior approval.

Technical Standards and Platform Requirements

1. Interoperability

Consent Manager platforms must be interoperable per standards notified by the Data Protection Board.
Common protocols/APIs will allow any Data Fiduciary to integrate seamlessly with multiple Consent Managers. - Users of different Consent Managers can interact with any Data Fiduciary without lock-in.
Anticipated creation of a Consent Manager network enabling cross-platform consent communication.
Early movers may benefit from network effects akin to UPI or Account Aggregator models.

2. Business Community

Redundancy and disaster recovery plans required to ensure continuous processing amid disruptions.
Compliance with Reasonable Security Practices per DPDP Rule 6 applicable to all data fiduciaries.

3. User Interface and Accessibility

Platforms must provide clear, plain-language consent notices separate from other content.
User experience should prioritize simplicity, clarity, multilingual support, and accessibility (e.g., for persons with disabilities)
Secure user authentication required, potentially including passwordless login, OTP, and two-factor methods.
Consent flows should be intuitive and independent from other platform functions.

4.Security and Data Protection Measures

End-to-end encryption ensures Consent Manager cannot read personal data in transit.
Comprehensive logging and monitoring of access, consent transactions, and system activity for 7-year retention.
Minimal data storage primarily for consent records and basic identification; pseudonymous identifiers preferred.
Secure API interfaces using mutual TLS, OAuth, and strict request validations. And regular security audits and penetration testing mandated.

5. Development and Compliance Timeline

Platforms should align early with draft standards before the Rule 4 obligations commence in November 2026.
Collaboration in industry sandboxes and early testing recommended for smooth implementation.

6. Privacy by Design

Consent Managers must limit data collection to necessities.
Provide privacy notices for user data held.
Obtain consent for any data processing beyond consent management services.
Compliance with standards like ISO 27001 is expected or may be mandated.

Obligations on Data Fiduciaries Using Consent Managers

RECOGNIZE AND ACT ON CONSENT VIA CONSENT MANAGERS:

- Consent given or withdrawn via a Consent Manager is legally binding on the Data Fiduciary (DF).
- DFs must integrate with standard APIs to receive valid consent tokens or withdrawal notices promptly.
- Timely cessation of data processing upon consent withdrawal is mandatory.

PRIVACY NOTICES AND CONSENT WORKFLOWS::

- Update privacy notices to inform users of their option to manage consent through Consent Managers.
- DFs must integrate with standard APIs to receive valid consent tokens or withdrawal notices promptly.
- Timely cessation of data processing upon consent withdrawal is mandatory.

INTEGRATION AND PARTNERSHIP DECISIONS

- DFs may build their own consent interfaces or partner with registered Consent Managers.
- Large firms must maintain independence in governance if investing or setting up Consent Managers
- 18 months compliance window (until May 2027) for full integration.

CONTRACTUAL ARRANGEMENTS

- Clear contracts delineating roles, liabilities, data security, breach notification, and indemnity are essential.
- Liability for Consent Manager errors usually rests with the Consent Manager, but coordination with DFs is crucial.
  Dispute resolution mechanisms should clarify responsibilities and processes.

DATA HANDLING AND SCOPE

- Consent Managers should be used only for necessary data and lawful purposes; no data collection loopholes.
- All consents must be free, specific, and lawful as per DPDP Section 6.

GRIEVANCE COORDINATION

- DFs must address complaints related to Consent Managers and coordinate resolution efforts.
- Both Consent Managers and DFs are responsible to respond to grievances within the stipulated deadlines.

NO FORCING OR EXCLUSIVITY

- DFs cannot compel users to use particular Consent Managers.
- Must honor valid consents from any registered Consent Manager equally, ensuring user choice.027) for full integration.

INTERNAL SYSTEMS AND READINESS

- IT systems must map and manage consents from Consent Managers securely and in real-time.
- Early resource allocation advised for smooth API integration and compliance.

CONTINUED RESPONSIBILITY

- Using Consent Managers does not absolve DFs from their direct obligations under the DPDP Act.
- DFs remain accountable for all processing on their behalf and must include consent management in audits and compliance.

SECTORAL COORDINATION

- Consents via sectoral systems (e.g., RBI's Account Aggregator, NDHM) must align with DPDP consent standards.
- Potential convergence or interoperability anticipated between sectoral and DPDP Consent Manager frameworks.

STRATEGIC OPPORTUNITY

- Early adaptation can enhance reputation as privacy-conscious and user-friendly.
- Consent Manager integration offers transparency and trust-building advantages.

Audit, Record-Keeping, and Reporting Expectations for Consent Managers under the DPDP Act

Both the regulatory framework and good governance dictate that Consent Managers maintain rigorous audit trails and compliance records. Below are the expectations on this front -

Consent Logs and Audit Trails	• Maintain detailed, immutable records of all consent activities for at least 7 years. • Logs must show all consents given, withdrawn, notices displayed, and data sharing events. • Records must be organized and searchable for transparency, compliance, and dispute resolution. • Use ledger-like databases or secure log management systems to ensure log integrity.
Internal Audits and Compliance Reviews	• Conduct regular internal audits (quarterly or annually) of systems and processes. • Audits cover security controls, operational workflows (e.g., consent handling, withdrawals), and legal compliance. • Outcomes of audits must be periodically reported to the Data Protection Board (DPB). • Maintain audit-friendly documentation like incident logs and compliance checklists.

Regulatory Reporting	• Notify the DPB and affected users promptly of personal data breaches, filing detailed reports within 72 hours. • Report any planned changes in control or mergers requiring Board approval. • Inform the Board about significant management changes, especially where conflict of interest concerns arise. • Submit periodic financial statements or net worth certificates (INR 2 Crore) as evidence of continued financial eligibility. • Provide usage statistics (user base, consent transactions) if requested by the Board for monitoring.or secure log management systems to ensure log integrity.
Transparency Reports	• Voluntarily publish annual transparency reports detailing consent transactions, grievance handling, government data requests, and resolution times. • Enhances trust and aligns with DPDP's transparency ethos.
Board Oversight and Inspections	• DPB has authority to conduct inquiries and onsite inspections, especially upon complaints. • Consent Managers must keep all audit reports, training records, compliance documents, and system configurations ready for inspection. • Having a designated Compliance Officer or team is advisable to interface with the DPB and manage reporting.

Grievance Records	• Maintain detailed logs of grievances including complaint nature, receipt date, resolution process, and timeline. • Publish grievance redressal policies and expected resolution timeframe (maximum 90 days). • DPB may review grievance records for compliance monitoring.
Retention Policy Audits	• Implement and audit retention and deletion policies ensuring data is not held longer than necessary, except mandatory 7+ year consent logs. • Delete personal data promptly when a user deletes their account, in line with policy.
Continuous Oversight	• DPDP mandates ongoing certification and compliance verification. • The Board can request information or take enforcement for non-compliance at any time. • Strong internal controls and continuous documentation are critical for avoiding penalties and ensuring smooth regulation.

This holistic set of audit, record-keeping, and reporting requirements ensures Consent Managers maintain high standards of accountability and transparency, essential for trust and compliance in the personal data ecosystem

Penalties and Consequences of Non-Compliance

Suspension or Cancellation of Registration

The Data Protection Board (DPB) can suspend or revoke a Consent Manager's registration for serious or persistent non-compliance.

Non-compliance examples: data misuse, undisclosed conflicts of interest, repeated security breaches, failure to maintain required INR 2 crore net worth

The Board may order transferring user consent records to another Consent Manager or notify Data Fiduciaries to cease reliance on the suspended entity.

Monetary Penalties by the Board

VIOLATION	PENALTY
Failure to implement adequate security safeguards.	Fine up to INR 250 Crore
Violations involving Data Principal rights or special provisions (e.g., children's data).	Fine up to INR 200 Crore
Administrative lapses or failure to comply with Board orders.	Smaller fines in Thousands or Lakhs
Breach of obligation on Consent manager	Fines up to INR 50 Crore per instance

Suspension or Cancellation of Registration

The Data Protection Board (DPB) can suspend or revoke a Consent Manager's registration for serious or persistent non-compliance.

Non-compliance examples: data misuse, undisclosed conflicts of interest, repeated security breaches, failure to maintain required INR 2 crore net worth

The Board may order transferring user consent records to another Consent Manager or notify Data Fiduciaries to cease reliance on the suspended entity.

Factors to determine the penalties are severity and duration of breach, intent, mitigation efforts and compliance history.

For Example: Unauthorised access to consent logs attracts potential multi-crore fine and remedial orders.

Collusion to obtain blanket consent also results in fines and possible suspension.

PENALTIIES ON INDIVIDUAL GREIVANCES	PENALTY ON DATA FIDUCIARY
Board may penalize Consent Managers for not addressing user grievances timely.	Data Fiduciaries can be fined (up to INR 50 Crore) for unlawful processing, including refusal to honor consent withdrawal via Consent Managers.
Fines related to failure to comply with Data Principal rights can be substantial (discretionary up to caps in the Act).	

Criminal Liability: The Act does not notably criminalise most violations.

- DPDP Act enforces penalties through regulatory actions
- Other laws may apply if fraud or criminal misconduct occurs.

Complaint and Redressal

Data Principals can complain to the Board against Consent Managers or Data Fiduciaries for non-compliance.

The Board can initiate investigations on complaints or systemic issues

Business Consequence

Beyond regulatory fines, non compliance can lead to business losses. Such as:

Suspension or deregistration disrupts operations and leads to loss of users and Data Fiduciary trust

Heavy fines, especially for startups, can be financially devastating.

Reputational damage can cause long-term loss of business in the privacy-focused Consent Manager ecosystem.

Enforcement Approach : Gradual enforcement from warnings to multi-crore penalties, and the Board has discretion to impose lesser fines or seek undertakings for corrective actions.

Illustrative cases for Consent Managers

The following cases illustrate the value proposition of Consent Manager in facilitating secure and user-controlled data sharing:

Non-Banking Financial Company (NBFC)

(Open Finance Scenario) - A NBFC or Fintech lender wants to evaluate a loan applicant's creditworthiness by looking at the applicant's bank statement or GST returns, which reside with another entity. Traditionally, the user might have to download PDFs or share login credentials, an inconvenient and risky process. With Consent Managers, this becomes seamless and compliant.

Step 1) Integration and User Registration

- An NBFC or fintech lender acting as a Data Fiduciary integrates its loan processing system with a registered Consent Manager platform, say "P".
- The user (Data Principal) registers on platform P, possibly leveraging national digital ID or simple signup.

Step 2) Consent Request Trigger

- When applying for a loan, the fintech triggers a consent request via P, specifying data required (e.g., 6 months of savings account statements from Bank Y) and purpose (loan processing).

Step 3) User Notification and Review

- The user receives a notification on P's app, showing detailed consent request information, data source, duration, purpose, and options to approve or deny.

Step 4) Consent Approval and Data Transfer

Upon approval, P orchestrates the transfer of encrypted bank statements:

- If the user holds data in a personal store (like DigiLocker) linked to P, the data is transferred directly to the fintech.
- If not, P routes consent to Bank Y (also onboarded as a Data Fiduciary), which, upon receiving the user's consent proof, securely shares the data with the fintech.

Step 5) Processing and Logging

- The fintech processes the loan application with the securely transmitted data.
- The Consent Manager logs all consent events, specifying user consent details and data sharing instances.

Step 6) Consent Withdrawal

- Post-loan approval, if the user wishes to revoke ongoing consent (such as monitoring), they use P's platform to withdraw consent.
- The Consent Manager notifies fintech NBFC X to cease data processing and periodic access.
- The withdrawal action is logged by the Consent Manager.

This use case shows how an NBFC and a bank can rely on a neutral Consent Manager to facilitate secure data portability with the user's explicit consent. It enhances user convenience and privacy. FinTech companies see a Consent Manager dashboard as a differentiator, allowing users to manage consents in one place.

Insurance Portability and Data Sharing

A customer wants to switch health insurance providers. The new insurer needs her past policy details and medical records to underwrite a policy. Traditionally, this may involve paperwork or lengthy processes. With a Consent Manager, the customer can authorize a smooth digital transfer:

Step 1) Consent Approval and Data Transfer

- Both the old insurer (Insurer A) and the new insurer (Insurer B) are onboarded onto Consent Manager platform “Q”.

Step 2) Processing and Logging

- The customer uses Q (perhaps integrated into Insurer B’s online portal via Q’s API) to issue a consent: “Share my claims history and policy details from Insurer A to Insurer B for the purpose of porting my insurance policy.”

Step 3) Consent Withdrawal

- Insurer A receives the consent request via Q and recognises the customer’s identity (through a linked account or identifier on Q). Because the customer’s consent is verified by the Consent Manager, Insurer A compiles the requested data (past claims, medical records, policy info) and sends it through the Consent Manager’s system to Insurer B.

Step 4) Consent Withdrawal

- Insurer B receives the data and completes the porting/underwriting process. The Consent Manager never saw the plaintext data, it simply facilitated the encrypted transfer.

Step 5) Consent Withdrawal

- The user’s dashboard on Q now shows that on date Y she gave consent for this transfer. If in the future she wants Insurer A to stop holding her data (assuming no legal need to retain), she could separately request deletion, but that aside, her immediate goal was achieved without hassle.

This exemplifies portability one of the consumer empowerment goals of DPDP. The user didn't have to chase Insurer A; the Consent Manager acted as her agent together data moved. It's analogous to mobile number portability but for personal data. Insurance companies benefit too: the process is automated and they obtain reliable data (direct from the source with consent logs attached, reducing fraud).

Healthcare and Medical Records Consent scenario

Use Case: A patient, X, visits a new specialist doctor. Her previous records (lab tests, scans) are with a hospital she visited earlier. Using a Consent Manager, she can allow the new clinic to fetch those records securely.

Step 1) The hospital and the clinic are participants in a Health Information Exchange network and also tied into a Consent Manager (possibly the ABDM itself or a similar platform could register as a Consent Manager). The patient has a Health ID and an account on the Consent Manager app.

Step 2) The specialist sends a consent request through the Consent Manager: "Dr. B (Clinic Y) requests access to your medical records from Hospital Z for providing you healthcare services (diagnosis/treatment)."

Step 3) X receives this request on her phone via the Consent Manager app. She sees Dr. B's details, what records are requested (say, all lab results from last 1 year at Hospital Z), and she approves for one-time access.

Step 4) Hospital Z's system, upon receiving the consent token, packages the relevant medical records. These might be PDFs or structured data, and sends them back via the Consent Manager to Clinic Y. Because of interoperability, this could happen near-instantly, and possibly integrated into the clinic's electronic health record system.

Step 5) Dr. B reviews the records and treats the patient. The Consent Manager logs that X gave consent on date M for this specific access which was used.

Step 6) The consent could be time-bound (many health consents might auto-expire after, say, 24 hours or a week). After that, Dr. B won't be able to pull further data without a new consent. X can also proactively revoke if she wishes (e.g. if some continuous access was granted for a care program, but she opts out later).

This health scenario is already being piloted. The ABDM's consent manager (called Health Information Provider/Consent Manager system) allows exactly this kind of exchange, and hospitals are guided to integrate it. For example, a hospital can use the ABDM consent manager to let patients digitally consent to share records with another hospital or an insurer. Under DPDP, such a consent manager would simply be one of possibly many. We might see independent health-tech companies becoming Consent Managers specializing in health data, or general-purpose Consent Managers handling health with necessary certifications (since health data might have additional safeguards).

Unified Consent Dashboard scenario for consumers in retail/e-commerce

Scenario: A user has given marketing consent to various e-commerce and telecom companies over time. She now wants to manage these in one place, perhaps withdraw some and keep others.

Step 1) The user signs up on a Consent Manager "C" and links her various service accounts (this linking could be via providing the email/phone she used on those services; the Consent Manager syncs consents via the services' APIs).

Step 2) On C's dashboard, she sees a list:
Company A – consent for newsletters (Active),
Company B – consent for data sharing with partners (Active),
Company C – no consent (Denied), etc., along with options to revoke.
This information is pulled because Company A, B, etc., as Data Fiduciaries, have either integrated or at least provided consent status to the Consent Manager when asked with proper auth.

Step 3) She decides to withdraw consent for Company B's data sharing. She toggles it off on the dashboard. C then transmits a withdrawal notice to Company B's systems. Company B is obligated to honor that and confirm cessation of that processing.

Step 4) She also sees an option to complain if any company is still bothering her after withdrawal. If, say, Company B continues a practice, she could raise a grievance via Consent Manager C's interface, which might route it to Company B's grievance officer or to the DPB if needed.

This cross-sector scenario highlights convenience: one app to rule them all, instead of managing 10 different account settings pages. It demonstrates how Consent Managers can serve as a privacy cockpit for users in the digital economy.

Government Services Data Sharing

Government agencies can leverage Consent Managers to securely and transparently process personal data, enhancing user control.

Scenario: A government scholarship portal needs to verify a student's income by accessing family income tax data.

- Instead of bespoke integrations, the portal routes data requests via a Consent Manager platform.

- The student (or parent) explicitly consents through the Consent Manager to share income tax data with the scholarship portal for eligibility verification.

- Data flows securely through the Consent Manager with all consent logged and potentially automatically revoked after use.

- This aligns with Section 7 of the DPDP Act, permitting legitimate data use while adding transparency by involving citizen consent wherever feasible.

- Common features across use cases include:

(a) Data sharing happens only with explicit individual consent.
(b) Digital consent replaces lengthy document processes, completing data transfers in seconds.
(c) Every transaction is recorded, supporting accountability.
(d) Consent specifies particular data and duration, minimizing unnecessary exposure.

Example: Employment background screening can use Consent Managers to get candidate consent for education record verification directly from universities, eliminating manual document collection.

- Businesses should consider integrating with existing Consent Managers rather than building proprietary consent modules, as a licensed ecosystem of Consent Managers is envisioned under DPDP.

- For users, this model makes tracking and controlling data sharing as convenient as online banking, reducing friction and enabling innovation based on trusted, consented data exchanges.

Conclusion

Consent Managers under the DPDP Act mark a significant evolution in India's data protection landscape, centralizing consent control and simplifying compliance while safeguarding user rights. Their interoperable, transparent, and secure platforms translate complex regulatory requirements into user-friendly experiences across diverse sectors. As India transitions into this new regime, Consent Managers will be instrumental in balancing innovation with rigorous privacy standards, ultimately enabling a harmonious and trustworthy digital economy where individuals retain meaningful control over their personal data.

Contact us

Ground Floor, 27-A, Hauz Khas Village,
New Delhi, 110016
Office: +91 11 41727676
info@akandpartners.in
www.akandpartners.in