PRODEVANS

Whitepaper · Volume 02

Consent Management Under DPDP

A complete guide for Indian enterprises

Understandingthe law,designing the platform,and preparing for May 2027

ZTrust

INSIDE THIS WHITEPAPER

CONTENTS

FIGURES

SECTION 01

THE SHIFT INDIA IS MAKING

For nearly two decades after India's digital economy began scaling rapidly, consent was treated largely as a procedural requirement. Users accepted privacy notices and terms of service as part of accessing digital platforms, while organisations focused primarily on enabling data collection and service delivery. The operational implications of consent management, including lifecycle governance, auditability, withdrawal handling, and purpose limitation, were rarely examined in a structured manner.

The Digital Personal Data Protection Act, 2023, along with the Digital Personal Data Protection Rules, 2025, fundamentally changes this model. Consent is no longer limited to a one-time legal acknowledgement; it becomes an operational requirement that must be consistently respected across systems, applications, business processes, and third-party data flows. Organisations are now expected to establish mechanisms for transparent notice delivery, granular consent capture, withdrawal management, rights handling, retention governance, and demonstrable compliance.

For many enterprises, this represents a significant operational and architectural shift. Achieving DPDP compliance requires more than updating privacy policies or introducing consent banners. It involves re-evaluating how personal data moves across the organisation, how consent records are maintained, how rights requests are fulfilled, and how evidence can be produced for regulators, auditors, and data principals. In practice, consent management becomes a cross-functional responsibility spanning legal, engineering, security, governance, and business operations.

This whitepaper examines consent management under the DPDP framework from an operational and implementation perspective. It covers the legal foundations of consent, lifecycle management, governance considerations, implementation architecture, operational risks, and phased adoption planning required to support sustainable compliance.

The focus throughout is on practical implementation considerations, operational readiness, and long-term governance sustainability under the DPDP framework.

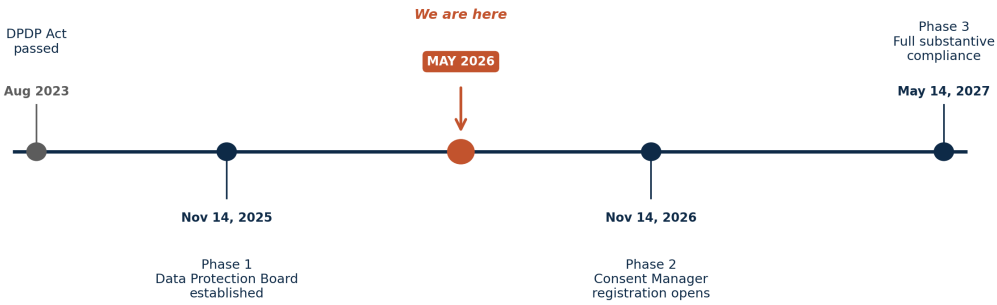
SECTION 02

DPDP AT A GLANCE

The Digital Personal Data Protection Act received Presidential assent on 11 August 2023. The accompanying DPDP Rules, 2025, which translate the Act into operational specifics, were notified on 13 November 2025. Together, they form the legal framework that now governs personal data in India. The Government has chosen a phased rollout, recognising that organisations need time to absorb the changes.

FIGURE 01

Three-phase rollout of the DPDP Act and Rules



Penalties of up to ₹250 crore apply once Phase 3 takes effect; full compliance is mandatory from 14 May 2027.

Figure 01 · The DPDP Act and Rules come into force in three stages, with full compliance required by May 2027.

THE THREE PHASES

Phase 1 took effect on 14 November 2025. The Data Protection Board of India, the regulator that will investigate complaints and impose penalties under the Act was established in the National Capital Region with four members. Phase 1 is largely about putting the institutional plumbing in place rather than imposing operational obligations on businesses.

Phase 2 takes effect on 14 November 2026. This is when the Consent Manager framework becomes operational: registered intermediaries can apply to the Board to act as Consent

Managers, the entities that will help data principals manage their consents across multiple data fiduciaries. The eligibility criteria and the technical interoperability standards apply from this date.

Phase 3 takes effect on 14 May 2027. This is the date that matters most for enterprises. From May 2027, the substantive obligations of the Act — notice and consent in their full form, the rights of data principals, breach notification, retention limits, the additional obligations on Significant Data Fiduciaries, and the rules on processing the data of children — all become enforceable. The penalty regime, with fines of up to ₹250 crore for serious violations, also takes effect.

WHAT IS IN SCOPE

The DPDP Act applies to the processing of digital personal data. "Personal data" is defined broadly: any data about an individual who is identifiable by or in relation to such data. "Digital" means data either collected in digital form, or collected on paper and later digitised. Data that is and remains on paper is not within the Act's scope, but in practice almost every organisation today digitises whatever it captures, so the practical reach is wide.

The Act applies extraterritorially. A company headquartered abroad that offers goods or services to data principals in India, and that processes their data in connection with that offering, is within scope regardless of where its servers are or where its processing happens. This mirrors the GDPR's reach and is one of several places where the DPDP framework consciously aligns with international practice.

Penalties under the Act are substantial. The Schedule to the Act prescribes fines of up to ₹250 crore (about USD 30 million) for the most serious failures — for instance, failure to take reasonable security safeguards when processing children's data. Lesser infractions attract correspondingly lesser amounts. The Board has the power to inquire into breaches on its own motion or in response to a complaint, and the decisions are appealable to the Telecom Disputes Settlement and Appellate Tribunal.

SECTION 03

THE CAST OF CHARACTERS

The DPDP Act introduces a vocabulary that is precise about who is doing what. Some of the terms will be familiar to anyone who has worked with the GDPR. Others, like Consent Manager and

Significant Data Fiduciary, are specific to the Indian framework. Getting these definitions right is not pedantry; the obligations of the Act fall differently on different roles, and confusing them is one of the easier ways to design a non-compliant system.

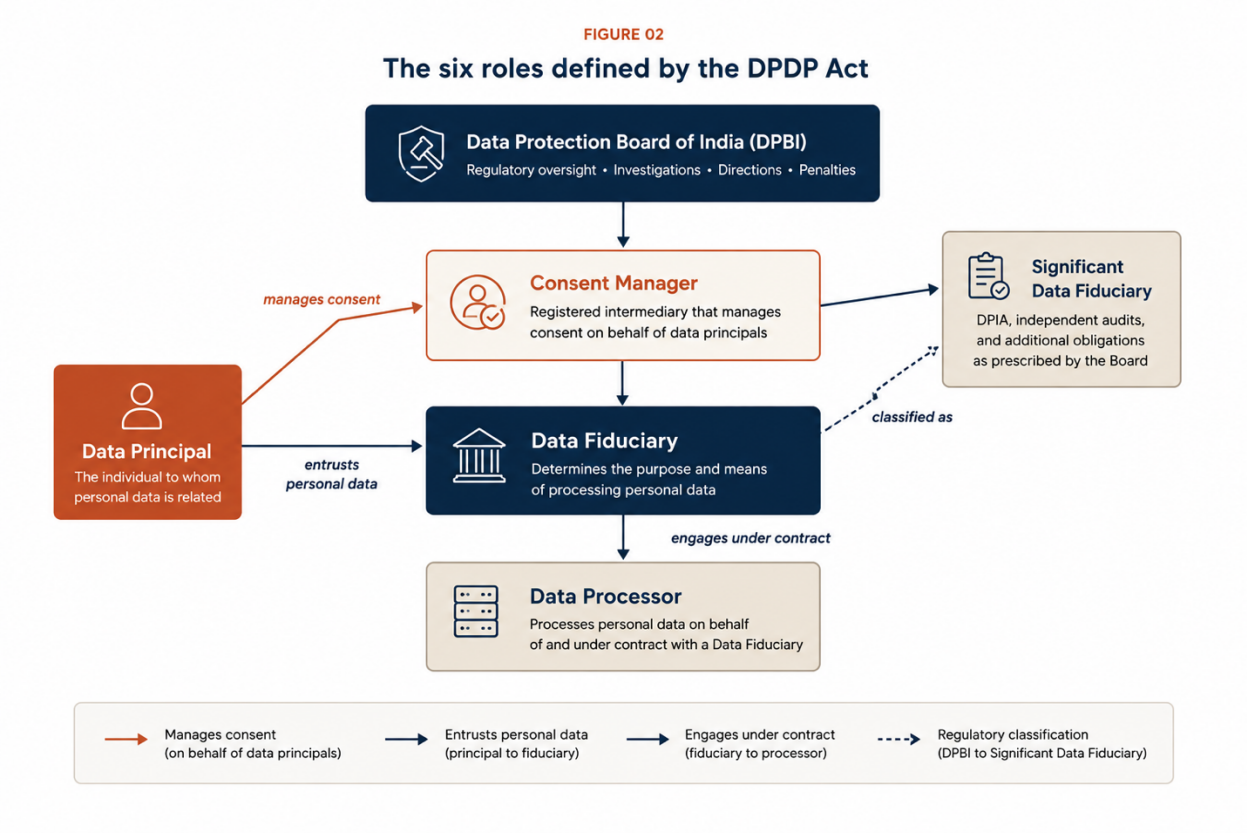


Figure 02 · Six roles work together to operationalise the DPDP framework.

Data Principal

The data principal is the individual to whom the personal data relates. In the GDPR vocabulary this is the data subject; the DPDP Act uses "data principal" to emphasise that the individual is the principal in the legal relationship and that data fiduciaries act on their behalf. A child's parent or lawful guardian, or the lawful guardian of a person with disability, also acts as the data principal in those cases.

Data Fiduciary

A data fiduciary is any person or entity that, alone or jointly with others, determines the purpose and means of processing personal data. The word "fiduciary" is deliberate: the Act characterises

the relationship as one of trust, not merely a commercial transaction. Most enterprises operating in India will be data fiduciaries with respect to at least some of the data they process — their customers' data, their employees' data, and so on.

Data Processor

A data processor processes personal data on behalf of, and under contract with, a data fiduciary. Cloud providers, analytics vendors, payment processors, customer-service outsourcers — these are typically processors when they work for a fiduciary. The fiduciary remains responsible to the data principal for what the processor does; the contract between fiduciary and processor must include reasonable security safeguards and other operational controls.

Significant Data Fiduciary (SDF)

The Government may designate certain data fiduciaries as Significant Data Fiduciaries based on factors set out in the Act : the volume and sensitivity of the data processed, the risk to the rights of data principals, the potential impact on the sovereignty and integrity of India, the risk to electoral democracy, the security of the State, and public order. SDFs face heightened obligations: appointing a Data Protection Officer based in India, conducting periodic Data Protection Impact Assessments, and undergoing periodic audits. The list of SDFs has not yet been notified at the time of writing.

Consent Manager

The Consent Manager is a distinctive Indian innovation. It is a registered intermediary that gives the data principal a single, interoperable interface to manage consents across many data fiduciaries. We devote Section 09 of this paper to the framework. The key point at this stage is that the Consent Manager is itself accountable to the data principal and is regulated by the Data Protection Board; it is not a vendor of the data fiduciary.

Data Protection Board of India

The Board is the regulator. Established under the Act and operationalised from 14 November 2025, it inquires into personal data breaches, hears complaints, mediates disputes, and imposes penalties for non-compliance. The Board's decisions are appealable to the Telecom Disputes Settlement and Appellate Tribunal, which provides a layer of judicial review. The Board's composition, powers, and procedures are set out in Chapter V of the Act and elaborated in the Rules.

SECTION 04

THE ANATOMY OF VALID CONSENT

Section 6 of the DPDP Act sets out what makes consent valid. The provision is short, almost terse, but every word in it carries weight. Consent must be free, specific, informed, unconditional, and unambiguous, given through a clear affirmative action. Each of those five qualities does independent work; missing any one of them invalidates the consent.

Figure 03 · The five pillars of valid consent under Section 6 of the DPDP Act.

FREE

Consent is free when the data principal can say no without losing access to the service they came for. A bank that withholds a savings account unless the customer agrees to receive third-party marketing is not collecting free consent for the marketing; the marketing consent has been bundled with the banking service, and the bundling makes the agreement coerced rather than voluntary. The test is straightforward: imagine the data principal answering "no" to the consent prompt. If, at that moment, they lose something they should have received anyway, the consent is not free.

The principle has consequences for product design. Marketing teams sometimes argue that bundling consent into the main service flow improves opt-in rates; that argument was always

commercially short-sighted, and under DPDP it is also legally invalid. Consent for each unrelated purpose has to be unbundled and presented as a genuine, separate choice.

SPECIFIC

Consent attaches to a purpose, not to a relationship. The same individual may interact with a single company in many capacities : as a customer, as a recipient of marketing communications, as an applicant for a loan, as a research subject in a product study and each of those processing activities requires its own consent. Specificity is what makes a partial withdrawal possible. A customer who consented to all four purposes and now wants to stop the marketing must be able to do so without losing the banking relationship.

Architectures that record consent as a single yes-or-no cannot deliver this; they treat consent as monolithic when the law requires it to be plural. The fix is to capture, store, and reason about consent at the level of the individual purpose, not the individual user.

INFORMED

Consent is informed when the notice that accompanies it tells the data principal, in language they can understand, what personal data is being collected, why, who it will be shared with, how long it will be kept, and how to withdraw. Rule 3 of the DPDP Rules makes the notice requirement concrete: a fair and reasonable description of the data, the purpose, the goods or services to be provided, the mode of exercising rights, and the means of grievance redressal.

The notice must be available in English and in any one of the languages listed in the Eighth Schedule of the Constitution that the data principal selects, twenty-two languages in all, from Assamese to Urdu. For a national enterprise, this is a non-trivial commitment. Notices must not only be translated but kept synchronised across languages whenever they change, and the data principal must be given a meaningful way to choose.

UNCONDITIONAL

Consent is unconditional when it is not tied to advantages, rewards, or features that should be available regardless. An e-commerce site that offers a discount only to users who agree to behavioural tracking is conditioning the agreement on an unrelated benefit. The data principal's decision to give consent has to flow from their genuine preference, not from a benefit that the business has artificially attached.

UNAMBIGUOUS, THROUGH CLEAR AFFIRMATIVE ACTION

Consent cannot be inferred from silence, from continued use of a service, from a pre-ticked checkbox, or from a default setting. The action that signals consent must be unmistakably an act of agreement, a button pressed, a switch flipped, a clear yes given. Burying the consent statement

inside a long terms-of-service document and asking the user to "accept the terms" is not unambiguous; the user is accepting the terms, not consenting to data processing.

In practice, this means that consent prompts should be visually and semantically separate from other agreements. They should ask one question at a time, in plain language, and require a deliberate response. The cost of a slightly longer onboarding flow is far smaller than the cost of having to recapture consents from the entire user base after an audit.

A NOTE ON 'LEGITIMATE USES'

Not every processing activity requires consent. Section 7 of the Act lists 'legitimate uses' that can serve as an alternative lawful ground: processing for the performance of a function under a law, for compliance with a judgment or court order, for responding to a medical emergency, for taking measures during a disaster, and for employment-related purposes. Distinguishing consent-grounded processing from legitimate-use processing at the design stage matters: asking for consent that is not legally required creates a downstream obligation to honour withdrawals that the enterprise may be unable to accommodate.

SECTION 05

NOTICE: WHERE CONSENT BEGINS

Consent without notice is not consent. Before the data principal can give a clear affirmative action, they must be told, in language they understand, what they are agreeing to. The notice is the foundation; everything that follows in the consent lifecycle is built on it.

WHAT THE NOTICE MUST CONTAIN

Section 5 of the Act and Rule 3 of the DPDP Rules together set out the minimum contents of a valid notice. The notice must describe the personal data that will be processed and the specific purpose for which it will be processed. It must list the goods or services or uses for which the data is needed. It must explain how the data principal can exercise their rights under the Act : the rights to obtain information, to correct, to erase, to lodge a grievance, and to nominate. And it must

provide a clear means by which the data principal can complain to the Data Protection Board if their concerns are not resolved.

Beyond these explicit elements, well-written notices today also include the retention period for the data, the categories of third parties with whom it may be shared, the means of withdrawing consent, and the contact details of the Data Protection Officer or other officer responsible for handling queries. None of these is strictly mandated by the minimum specification, but each becomes essential as a matter of trust and transparency, and each tends to be expected by sophisticated data principals.

THE LANGUAGE REQUIREMENT

The notice must be available in English and in any one of the twenty-two languages listed in the Eighth Schedule of the Constitution that the data principal selects. The Act gives the data principal the choice of language; the data fiduciary cannot force English on a user whose first language is Tamil or Punjabi. For most enterprises, this is the single most under-estimated requirement in the Act. It is not enough to have a translation; the translation must be accurate, must be updated whenever the English version changes, and must be served correctly based on the user's selection.

The operational implications run deep. Notices need to be versioned and addressable, so that every consent record can be traced back to the exact text the data principal saw at the moment they agreed. Translation workflows need to be on a single source of truth, so that an update to the English notice does not leave eleven other versions stale. And the notice management system needs to be auditable: a regulator inquiring about a consent record will want to see not only the text, but the date it was active, the language served, and the chain of revisions that led to it.

PLAIN LANGUAGE IS A PRODUCT PROBLEM

A notice that is technically compliant but written in dense legal prose fails the spirit of the law and, increasingly, also fails its letter. The Act's requirement that consent be "informed" presupposes a data principal who has actually understood what they are agreeing to. A nineteen-year-old onboarding to a payments app on a budget phone, scrolling through a notice on a small screen, is the realistic test case. If they cannot follow the notice, the consent is not informed, no matter what the lawyers have written.

Treating notice design as a product problem rather than a legal one is the practical fix. The legal team owns the substance; the product team owns the form. Plain language, short sentences, clear visual hierarchy, layered disclosure (an overview followed by expandable details for those who want more), and accessible design — these are the things that turn a notice from a formality into an actual exchange of information.

SECTION 06

THE CONSENT LIFECYCLE

Consent is not a state. It is a process that runs alongside the data lifecycle for as long as the data exists, and continues for the retention period required for evidence even after the data has been erased. Treating consent as an event, a moment of agreement that is captured and forgotten is the single most common architectural mistake we see in pre-DPDP organisations. The seven stages below describe the lifecycle as it has to be operationally implemented.

FIGURE 04

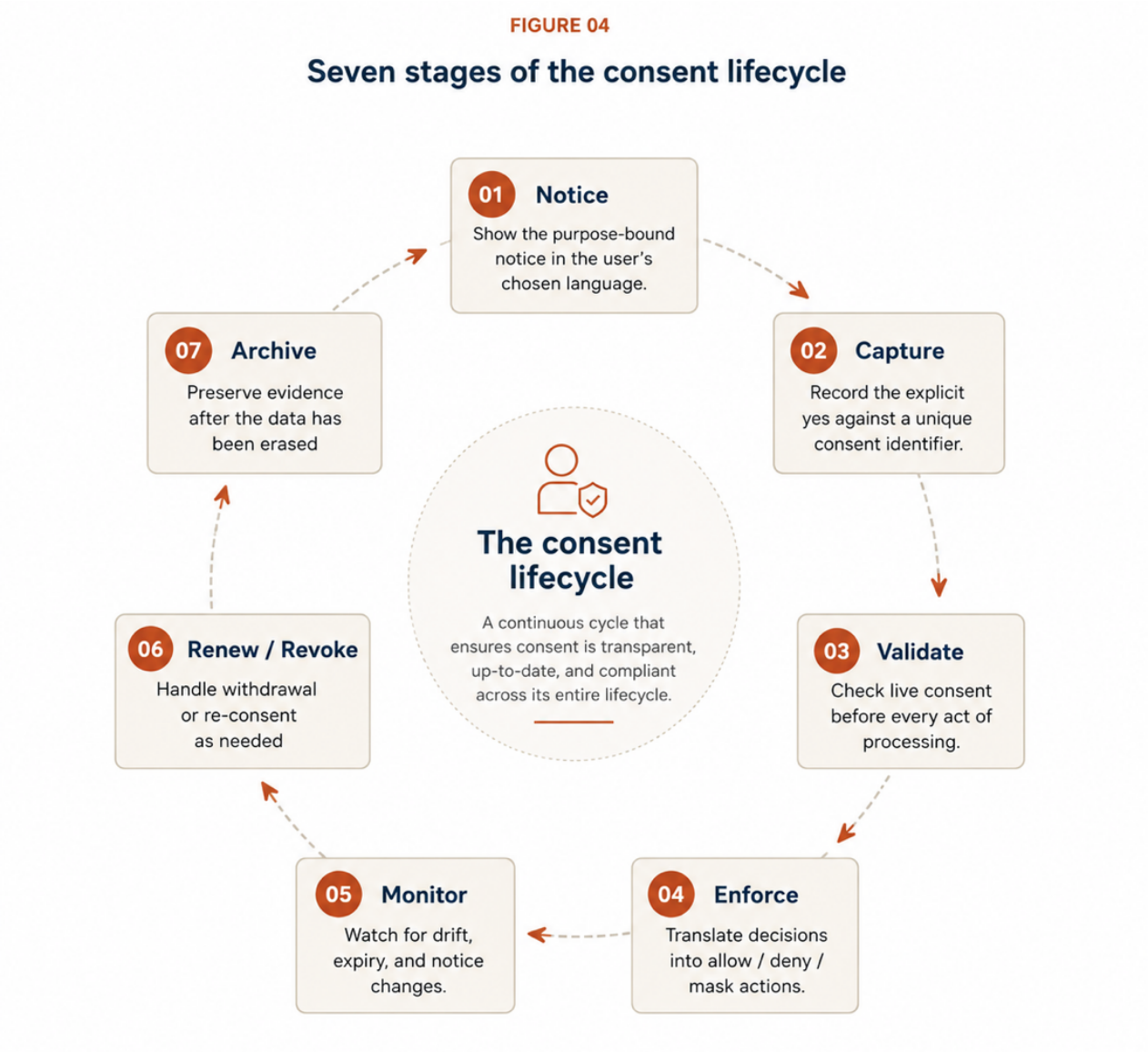


Figure 04 · The consent lifecycle is continuous, not a one-time event.

01	**Notice** A purpose-bound notice is shown to the data principal in their chosen language. The notice declares what data will be processed, the purpose, the recipients, the retention horizon, and the mechanisms for withdrawal and grievance. The notice is versioned and addressable; every consent collected can be traced back to the exact text the data principal saw at the moment they agreed.
02	**Capture** The data principal performs a clear affirmative action. The system records the action, the timestamp, the channel, the device fingerprint where available, the notice version shown, and the specific purposes consented to. Each capture event produces a unique consent identifier that becomes the durable handle for everything that follows.
03	**Validate** Before any processing system uses personal data, it asks the consent layer whether a valid consent exists for the specific purpose, the specific data principal, and the specific data category. Validation is not a one-time check at intake; it is an ongoing question asked at every meaningful processing event. If validation fails, the operation does not proceed.
04	**Enforce** Validation alone does not stop misuse. Enforcement translates a consent decision into a system action: routing, masking, redaction, denial, or downstream propagation. Enforcement is what makes consent something the rest of the architecture cannot work around, even by accident, even under deadline pressure.
05	**Monitor** Consents have a half-life. Notices change. Purposes evolve. Retention horizons expire. The monitoring stage watches for these drifts and flags consents that are about to lapse, that no longer match the active notice, or that have been left orphaned by a process change. Monitoring is what keeps the consent estate from quietly going stale.

06	**Renew or revoke** When a data principal withdraws consent, or when a notice changes materially enough to require re-consent, the lifecycle returns to its first stage. The platform must support partial revocation — stopping marketing while preserving the customer relationship — and must propagate the revocation to every downstream system that holds the data, with an auditable trail of when each system acknowledged the change.
07	**Archive** Even after consent is withdrawn and the underlying data is erased, the record of the consent itself must persist for the period required to demonstrate compliance. The archival stage preserves an immutable record of what was consented to, when, by whom, and on what basis it ended. This is the evidence layer the platform offers to auditors, to regulators, and to the data principal who returns months later asking what happened to their data.

SECTION 07

RIGHTS OF THE DATA PRINCIPAL

The Act gives every data principal a set of rights that they can exercise against any data fiduciary that processes their personal data. The rights are not theoretical: from May 2027, when Phase 3 takes effect, the data fiduciary is operationally obliged to honour them, with prescribed timelines and enforcement consequences for failure. An enterprise that has not built the workflows to handle these rights at scale will find itself unable to respond when the requests start coming in.

THE RIGHT TO INFORMATION

Every data principal can ask a data fiduciary to confirm whether their personal data is being processed, to receive a summary of the data being processed and the processing activities undertaken, and to be told the identities of any other data fiduciaries or processors with whom the data has been shared along with a description of what was shared. This is the foundation of accountability; without it, the other rights are exercises in the dark.

Operationally, this means the enterprise needs to be able to assemble, on request, a coherent picture of a single data principal's data across every system that holds any of it. For a large bank with dozens of internal systems and many third-party vendors, this is non-trivial. The work has to start with a data inventory and end with a tested workflow that can produce the report within the timelines the data principal expects.

THE RIGHT TO CORRECTION, COMPLETION, UPDATING, AND ERASURE

A data principal can ask the data fiduciary to correct inaccurate or misleading personal data, to complete data that is incomplete, to update data that has become out of date, and to erase data that is no longer necessary for the purpose for which it was collected. Each of these is a separate operational workflow with separate engineering implications.

Erasure is the most operationally demanding. When a data principal asks for their data to be erased and they have no contrary obligation to retain it, the data must be erased not just from the primary system but from every replica, every backup that is not currently in cold archive, and every downstream system that received it. The Act does not exempt complex enterprise architectures from this requirement; it presumes that data fiduciaries have built systems that can comply.

THE RIGHT OF GRIEVANCE REDRESSAL

Every data fiduciary must provide a readily available means by which a data principal can complain about the way their data is being handled. The Rules require that grievances be resolved within a reasonable period and no later than ninety days. This is a hard deadline; the draft Rules had left it to the discretion of the fiduciary, but the final Rules have closed that flexibility.

The ninety-day clock starts when the grievance is received, not when it is acknowledged. Most enterprises will need to designate a grievance officer, build a tracking system that can demonstrate compliance with the timeline, and ensure that the workflow is genuinely available to data principals, not buried behind an unmonitored email address.

THE RIGHT OF NOMINATION

A data principal can nominate another individual who will be able to exercise the data principal's rights in the event of their death or incapacity. This is novel in international comparison; few other jurisdictions have an equivalent. Operationally, it means the data fiduciary needs a mechanism to record and verify the nomination, to retain it alongside the data principal's other consents and preferences, and to honour it when the situation arises.

In practice the nomination right will be exercised in a small minority of cases, but the system has to be built for the cases when it is. For sectors like banking, insurance, and healthcare, where the

question of who is entitled to act on behalf of an incapacitated or deceased person is operationally familiar, the framework should integrate cleanly with existing processes.

SECTION 08

SPECIAL CASES: CHILDREN AND PERSONS WITH DISABILITIES

Section 9 of the DPDP Act sets out a separate regime for the personal data of children and of persons with disabilities. The provisions are protective: they recognise that consent given by a person who lacks the legal or factual capacity to evaluate it cannot be relied upon, and they place additional obligations on the data fiduciary to verify, to restrict, and to behave with care.

WHO COUNTS AS A CHILD

Under the Act, a child is an individual who has not completed eighteen years of age. This is the same definition that applies in most other Indian statutes, but it is higher than the equivalent threshold in many other jurisdictions: under the GDPR, the default age below which children's data has special protection is sixteen, with member states able to lower it to thirteen. India's eighteen is the cleanest possible alignment with the broader legal framework, and it has significant operational consequences for any service whose user base includes adolescents.

VERIFIABLE PARENTAL CONSENT

Before processing the personal data of a child, the data fiduciary must obtain verifiable consent from the parent or lawful guardian. The Rules elaborate on what verifiable means: the consent must be capable of being demonstrated through reliable methods, and the data fiduciary must take steps to confirm that the person giving consent is indeed the parent and is an adult. The practical methods are still being worked out in industry guidance; they include cross-referencing identity documents, using digital signatures backed by trusted services, and integrating with the Government's digital identity infrastructure where appropriate.

Verification is genuinely hard. A teenager who wants to use a service can easily mis-state their age; a parent's identity can be forged. The Act does not require absolute certainty, but it does require reasonable measures, and the standard is high enough that ad-hoc click-through verification (a checkbox that says "I am the parent") almost certainly does not meet it.

PROHIBITED PROCESSING

Even with verifiable parental consent, certain kinds of processing of children's data are simply prohibited. The Act forbids tracking, behavioural monitoring, and targeted advertising directed at children. This is an outright ban, not a consent-overcome restriction. A service that, for example, profiles user behaviour to recommend content is operating differently when its user is a minor: the recommendation engine has to be configured not to do so. The same applies to advertising networks; their targeting models cannot use children's data even if a parent has technically consented.

The penalty for violating these specific prohibitions is among the highest in the Act. Section 33 prescribes a fine of up to ₹200 crore for breach of additional obligations relating to children's personal data. For a service that knowingly tracks teenagers, the financial exposure is real.

PERSONS WITH DISABILITIES

The Act extends the parental consent regime to persons with disabilities who have a lawful guardian. The lawful guardian gives consent on behalf of the data principal. The framework is otherwise similar: the consent must be verifiable, the guardian must be lawfully appointed, and the protective restrictions apply. Healthcare, social services, and education are the sectors where this provision will be most operationally relevant.

SECTION 09

THE CONSENT MANAGER FRAMEWORK

The Consent Manager is one of the most distinctive features of the Indian framework. Most international data protection laws place the burden of consent management on each individual data fiduciary; a citizen who deals with twenty different companies has to manage twenty different consent relationships, on twenty different interfaces, with twenty different ways of withdrawing. The DPDP Act takes a different approach. It creates a third-party intermediary, the Consent Manager that gives the data principal a single, interoperable platform to manage all their consents.

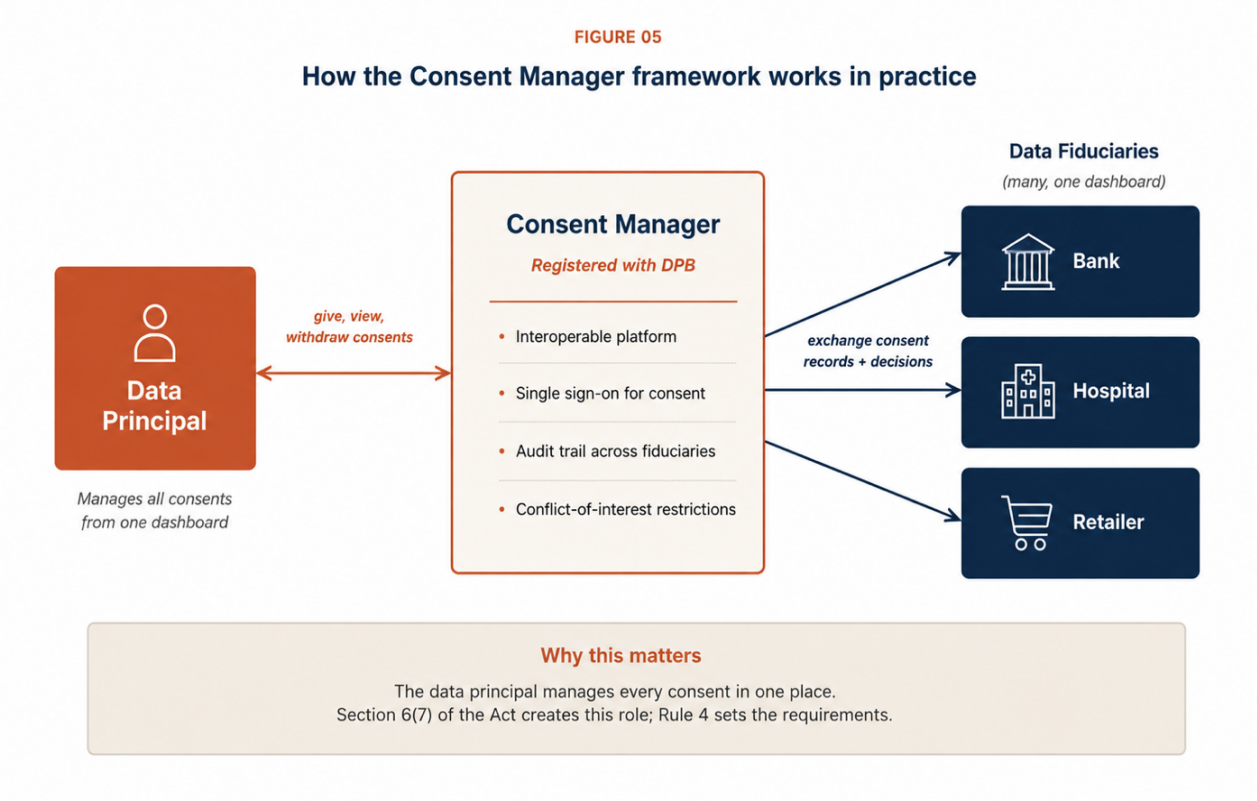


Figure 05 · A Consent Manager sits between the data principal and many data fiduciaries.

HOW IT WORKS

Section 6(7) of the Act creates the role: a data principal may give, manage, review, or withdraw their consent through a Consent Manager registered with the Data Protection Board. From the data principal's perspective, the Consent Manager is a dashboard. They sign in, they see all the consents they have given to all the data fiduciaries they have dealt with, and they can adjust any of them, grant a new consent, withdraw an existing one, change the scope, see the history.

From the data fiduciary's perspective, the Consent Manager is an integration. The fiduciary connects to one or more Consent Managers through standardised APIs and receives consent decisions in a uniform format. When a data principal withdraws a consent through their Consent Manager, the fiduciary receives a notification and is obliged to act on it just as it would on a direct withdrawal.

Eligibility and obligations

Rule 4 of the DPDP Rules sets out who can register as a Consent Manager. The applicant must be a company incorporated in India. It must have a minimum net worth of ₹2 crore (approximately USD 225,000). It must be independently certified as meeting interoperability and security standards. And it must avoid conflicts of interest with data fiduciaries — its directors, key personnel, and senior management cannot have material pecuniary relationships with the fiduciaries it serves.

The conflict-of-interest restrictions are intended to ensure that the Consent Manager is genuinely working for the data principal, not as a proxy for the fiduciaries. A consent dashboard run by a bank, for the bank's own customers, with the bank's commercial interests embedded in its design, would defeat the purpose of the framework. The Act's answer is to insist on structural independence.

Why this matters for enterprises

Even if your organisation is not planning to become a Consent Manager, you will almost certainly need to integrate with one or more of them. A data principal who manages their consents through Consent Manager X expects you to receive their decisions from Consent Manager X. Your consent management platform needs to speak the standardised protocol, accept inbound consent events, propagate them to your processing systems, and acknowledge them back to the Consent Manager.

Phase 2 of the rollout, which begins on 14 November 2026, opens the registration window. Enterprises that plan to build or partner with Consent Managers need to be ready by then; enterprises that will simply integrate with them need to plan integration work into their 2026-27 roadmaps. The standardised APIs are still being finalised; following the DPB's guidance and the published technical standards as they emerge will be essential.

SECTION 10

Practical implementation essentials

Translating the obligations of the DPDP Act into a working platform requires a number of building blocks. Some of these will already exist in mature enterprises, in some form; most will need to be designed, integrated, or replaced. The list below is not exhaustive, but it captures the components that we consistently see in implementations that pass review and avoid the most common pitfalls.

A NOTICE RENDERING AND TRANSLATION LAYER

This is the front-of-house system that presents notices to data principals in their chosen language at the right moment in their journey. It needs to support multiple languages from the Eighth Schedule, to version notices independently of the user interfaces that display them, and to track which version of which notice was shown to which data principal. Without this versioning, every consent record loses its evidentiary value the moment the notice changes.

A CONSENT VAULT

The vault is the system of record for consent events. It stores, for each consent, the unique identifier, the data principal's identity, the purpose, the notice version shown, the timestamp, the channel, and the current state. The vault should be append-only — every change generates a new event rather than overwriting an old one — and ideally cryptographically verifiable, so that the integrity of the record can be demonstrated to an auditor.

A POLICY ENGINE FOR PURPOSE BINDING

The policy engine translates the human-readable purpose described in the notice ("use my data for credit-card marketing") into a machine-readable policy that processing systems can evaluate ("allow access to credit-card-related data for the marketing service, but deny access to mortgage-related data"). Without this layer, the consents in the vault are decorative; the processing systems have no way to know what they imply.

A DATA PRINCIPAL SELF-SERVICE PORTAL

This is the parity-of-effort surface. Whatever a data principal can do to give consent, they must be able to do, with equal ease, to view, modify, or withdraw it. The portal is also the place where they exercise their rights under the Act — to request information, to ask for correction or erasure, to lodge a grievance, to nominate. A good portal makes these flows fast and clear; a bad portal becomes the single largest source of regulatory complaints.

A DPO CONSOLE AND AUDIT LAYER

Internal users — the Data Protection Officer, the legal team, the security team — need a working view of the consent estate. Volumes of capture and withdrawal, expiring notices, pending grievances, jurisdictions of data principals, evidence bundles for specific individuals. This layer turns compliance from a quarterly artefact into an operational dashboard.

AN INTEGRATION SURFACE

The richness of the APIs, SDKs, and event streams that connect the consent platform to the rest of the enterprise determines whether the platform is a central authority or just another silo. Every system that processes personal data — the CRM, the core banking platform, the marketing

automation suite, the data warehouse — needs to be able to ask the platform for decisions and to receive notifications when consents change.

Consent Manager interoperability

From November 2026, the platform must speak the standardised protocols used by registered Consent Managers. The technical specifications are emerging through DPB notifications and industry working groups; staying current with them and designing for interoperability from the start will save significant rework later.

SECTION 11

Common pitfalls

The patterns described below appear in nearly every consent management programme that goes wrong. They are not exotic. They are predictable, and naming them clearly is the best way to avoid them at design time rather than discover them at audit time.

The bundled 'yes'

All purposes are stacked into a single consent prompt. The data principal cannot choose to consent to one and decline another. The architecture downstream has no way to honour partial withdrawal because no granular record exists. This is the most expensive failure mode to correct, because rectification requires recapturing consent from the entire user base after the architecture has been redesigned to support specificity.

The opaque purpose

Purposes are written in language so general that they admit any future use: "service improvement," "business operations," "related services." The notice technically discloses something, but the data principal cannot have given specific consent because no specific purpose was ever stated. Regulators read these clauses as evidence of bad faith, not as evidence of consent.

The asymmetric exit

Consent capture is a button. Withdrawal is an email to a help desk that takes three working days. The Act's parity-of-effort principle explicitly forbids this asymmetry. It is one of the most visible signals to a regulator that an enterprise is not serious about its obligations, and the architectural fix i.e putting withdrawal in the same self-service surface as capture is among the easier remedies.

The orphaned record

Consent is captured by the front end and stored in a database, but no system downstream is checking it before processing. The vault fills up. The enforcement layer was never built. The data flows continue exactly as they did before. The enterprise believes it has consent management because it has a database of consents; in practice, the consents are doing nothing. This is the single most common failure mode in enterprises that bought a consent product and never changed how their applications work.

The frozen platform

The platform is built once, deployed, and then never updated. Notices are not re-versioned when terms change. New systems are integrated outside the platform because going through it is too slow. After eighteen months, the platform represents the data flows of a year and a half ago. The fix is governance: make the platform a required path for every new system that touches personal data, and instrument the path so that the friction is visible and reducible.

Treating it as a one-time project

This is the meta-failure that underlies most of the others. Compliance with DPDP is not an event with a finish line in May 2027; it is a continuing obligation that will track the enterprise for as long as it processes personal data. Programmes scoped as one-time projects produce platforms that fall behind the moment the project closes. The enterprises that fare best treat consent management the way they treat security: as a property of how they build software, owned by a permanent function with a budget and a roadmap.

SECTION 12

A roadmap from today to May 2027

With twelve months between today and the substantive enforcement deadline, an enterprise that has not yet started will need to move with discipline. The roadmap below sets out what we recommend across the next year. Organisations that are further along can use it as a checklist; those just starting can use it as a sequence.

Q2 2026	**Inventory and gap assessment** Map personal-data flows across the enterprise, including data categories, purposes, systems, third parties, and retention periods. Identify gaps between current practices and DPDP requirements, and create a prioritised remediation backlog.
Q3 2026	**Governance, design, vendor decisions** Establish programme ownership, governance, and reporting structures. Design multilingual notices with legal teams, and decide whether to build, buy, or extend a consent platform. If partnering with vendors, begin procurement early to account for enterprise integration timelines.
Q4 2026	**Build, pilot, integrate with Consent Managers** Begin platform implementation or vendor integration as Consent Manager registration and technical standards become operational. Run pilots on selected customer journeys to validate consent capture, DPO workflows, and self-service experiences end to end.
Q1 2027	**Enterprise rollout and audit preparation** Extend consent management across systems handling personal data, prioritising high-risk environments and third-party sharing workflows. Begin audit readiness testing to validate evidence generation, consent traceability, and operational integrity.
May 2027 +	**Continuous compliance** With the Act becoming enforceable, consent governance shifts from a project to an ongoing operational capability. Re-consent flows, withdrawal handling, grievance management, and consent integrations become part of regular enterprise processes.

SECTION 13

IN CLOSING

The DPDP Act introduces a significant shift in how organisations govern and operationalise personal data. Consent management is no longer limited to compliance documentation or consent interfaces; it now requires scalable systems capable of managing consent capture, validation, enforcement, withdrawal, monitoring, and auditability across business functions and digital platforms.

This whitepaper has outlined the key components of an effective consent management programme, including governance, lifecycle management, implementation architecture, and operational considerations. While implementation approaches may vary across organisations, the principles of transparency, accountability, interoperability, and auditability remain central to sustainable DPDP compliance and long-term customer trust.

ABOUT SWIKRUTI

Swikruti by ZTrust helps enterprises implement DPDP-aligned consent management through a unified framework for consent capture, validation, enforcement, monitoring, and auditability across systems and channels.

Designed for interoperability and enterprise-scale deployment, the platform enables organisations to build transparent, manageable, and regulation-ready consent operations.

OPERATIONALISE CONSENT GOVERNANCE WITH SWIKRUTI

EXPLORE SWIKRUTI