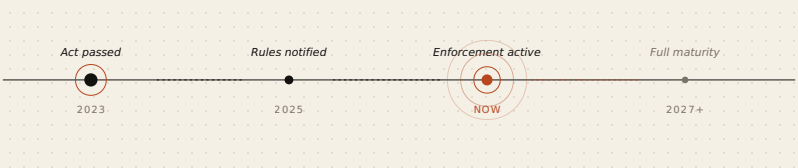
PUBLISHED BY
Prodevans
Technologies

VOL. 01 · APRIL 2026
WHITEPAPER
DPDP COMPLIANCE

A DEFINITIVE GUIDE FOR INDIAN ENTERPRISES

The DPDP Compliance *Guide.*

Obligations, consent architecture, and a practical readiness framework for Data Fiduciaries operating under India's Digital Personal Data Protection Act.



PUBLISHED BY
Prodevans Technologies

PLATFORM
ZTrust · Swikruti

EDITION
Volume 01 · April 2026

00

EXECUTIVE SUMMARY

The Digital Personal Data Protection Act is *no longer a future concern.* With rules notified in 2025 and enforcement now active, Indian enterprises face penalties of up to ₹250 crore per instance — and a compliance surface that no off-the-shelf policy can cover.

This document is written for the compliance leaders, CISOs, General Counsels, and product heads tasked with operationalising DPDP inside complex organisations. It maps the eight core obligations, isolates the deltas for teams already running GDPR programmes, and breaks down why consent — treated casually in most implementations — is the single largest source of compliance failure.

The final section presents a readiness maturity framework, the four architectural layers a defensible compliance stack requires, and how **ZTrust by Prodevans** — with its Swikruti consent module at the core — helps operationalise each of them.

CHAPTER 01 · THE MOMENT

India's data privacy moment: why DPDP *changes everything.*

India processes more personal data than almost any country on earth. Until August 2023, it did so without a comprehensive privacy law. That era is over.

The Digital Personal Data Protection Act, 2023 is the culmination of nearly a decade of legislative effort — from the 2017 Puttaswamy judgment that elevated privacy to a fundamental right, through three successive draft bills, to the Act now in force with rules notified and a Data Protection Board constituted. For enterprises that previously treated privacy as a matter of reputational hygiene, the Act introduces a mandatory operating discipline backed by financial consequences measured in the hundreds of crores.

What makes DPDP consequential is not its existence but its surface area. The Act applies to any entity that determines the purpose and means of processing personal data of individuals in India — whether the entity is incorporated here or not. It also reaches global processing that targets Indian users, and explicitly overrides inconsistent provisions of other existing laws. For a digital economy approaching one trillion dollars, that scope covers virtually every commercial data flow: onboarding, marketing, analytics, payments, logistics, HR. No business above a trivial scale is outside it.

900M+	₹250Cr	08
ACTIVE INDIAN INTERNET USERS	MAXIMUM PENALTY PER INSTANCE	CORE OBLIGATIONS ON EVERY DATA FIDUCIARY

KEY DEFINITIONS

Data Fiduciary	Any person who — alone or jointly — determines the purpose and means of processing personal data. The DPDP equivalent of a Controller under GDPR, but with fewer lawful bases available.
Data Principal	The individual to whom the personal data relates. In the case of children, includes lawful guardians. Data Principals hold rights of access, correction, erasure, grievance redressal, and nomination (Sections 11–15).
Personal Data	Any data about an individual who is identifiable by or in relation to such data. The Act does not create a separate category for "sensitive" personal data — a material simplification from GDPR.
Significant Data Fiduciary	A class of Fiduciary notified by the Central Government based on volume and sensitivity of data, risk to electoral democracy, security of the State, and other factors. Subject to additional obligations including DPO appointment and DPIAs.

The practical implication is that compliance is no longer a document to be drafted and filed. It is a continuous operational programme that must span product, engineering, security, legal, and customer operations — and that must be demonstrable to regulators at any moment.

CHAPTER 02 · THE OBLIGATIONS

Key obligations under the DPDP Act: *a structured overview.*

Eight obligations sit at the core of every Data Fiduciary's compliance posture (Sections 4–10). Each is individually straightforward. Operationalised together, at enterprise scale, they are the hardest engineering problem most compliance programmes have ever faced.

The obligations are not a checklist to be ticked once. They are commitments the Fiduciary must be able to demonstrate at every moment of a data lifecycle — from collection through to erasure — and across every downstream processor. The Act's penalty schedule does not reward best effort. It prices specific failures.

NO.	OBLIGATION	WHAT IT REQUIRES	PENALTY EXPOSURE
01	Consent	Free, specific, informed, unconditional, unambiguous consent obtained through a clear affirmative action, with the right to withdraw at any time.	Up to ₹200 crore
02	Notice	A standalone notice — in English and 22 scheduled languages — describing data collected, purpose, rights, and grievance mechanism before or at the time of collection.	Up to ₹50 crore
03	Purpose Limitation	Data processed only for the specific purpose disclosed in the notice and consented to. New purposes require fresh notice and consent.	Up to ₹200 crore
04	Data Minimisation	Only personal data necessary for the stated purpose may be collected. Excess collection is itself a violation, regardless of subsequent handling.	Up to ₹200 crore

NO.	OBLIGATION	WHAT IT REQUIRES	PENALTY EXPOSURE
05	Storage Limitation	Erase personal data once the purpose is served or consent is withdrawn, unless retention is required by law. Erasure must propagate to processors.	Up to ₹200 crore
06	Accuracy	Ensure data is complete, accurate, and consistent — particularly where used for decisions affecting the Data Principal.	Up to ₹50 crore
07	Security Safeguards	Implement reasonable security measures — encryption, access control, logging — to prevent breach. Notify the Board and affected Principals within 72 hours of any personal data breach.	Up to ₹250 crore
08	Grievance Redressal	Publish contact details of a grievance officer. Acknowledge and resolve complaints within 90 days before they can be escalated to the Data Protection Board.	Up to ₹10 crore

Penalty figures reflect the maximum under the First Schedule of the Act. The Board may impose penalties below these caps based on gravity, duration, and cooperation. Multiple obligations may be breached in a single incident.

The compounding nature of failure

A single defective consent flow typically breaches at least three of these obligations simultaneously — Consent, Notice, and Purpose Limitation. This is why fragmented compliance work, where teams address one obligation at a time, tends to understate both effort and exposure. The obligations are interdependent; a programme is only as strong as its weakest link.

CHAPTER 03 · THE DELTAS

DPDP vs GDPR: what Indian enterprises with global operations *need to know.*

For enterprises already operating a GDPR programme, the instinct to lift-and-shift is natural — and incorrect. DPDP is philosophically adjacent to GDPR but materially different in the provisions most likely to create enforcement exposure.

What follows is not a comprehensive comparison. It is the set of deltas that require active engineering and policy changes, not paperwork updates. Teams that assume GDPR compliance translates automatically will find themselves exposed on consent, on children's data, and on cross-border transfer architecture in particular.

DIMENSION	DPDP 2023	GDPR
Lawful bases for processing	Consent, plus a closed list of "Legitimate Uses" (employment, emergencies, state functions, compliance with law). Legitimate interest is **not** a basis.	Six lawful bases including consent, contract, legal obligation, vital interests, public interest, and **legitimate interests** (with balancing test).
Consent standard	Must be free, specific, informed, unconditional, unambiguous, given through clear affirmative action, and in plain language across 22 scheduled languages.	Must be freely given, specific, informed, and unambiguous. Plain language required. Multi-language support not mandated.
Children's data	**Under 18 years** requires verifiable parental consent. Tracking, behavioural monitoring, and targeted advertising to children are prohibited.	**Under 16 years** (member states may lower to 13). Specific protections apply but no blanket ban on tracking.

DIMENSION	DPDP 2023	GDPR
Cross-border transfer	**Negative list approach:** transfers permitted unless to a country specifically restricted by the Central Government. Sectoral laws may impose further restrictions.	**Adequacy-based:** transfers only to adequacy-listed countries or with additional safeguards (SCCs, BCRs, derogations).
Data Protection Officer	Mandatory only for Significant Data Fiduciaries as notified by Government. DPO must be based in India.	Mandatory for public authorities, large-scale monitoring, and processing of special categories. Can be internal, external, or EU-wide.
Maximum penalty	**₹250 crore per instance** of breach, per violation category. No turnover-linked cap.	**€20 million or 4% of global annual turnover**, whichever is higher.
Individual rights	Access, correction, erasure, grievance redressal, nomination. **No explicit right to data portability or to object.**	Access, rectification, erasure, restriction, portability, object, and rights related to automated decision-making.

The three provisions that demand engineering work

For teams triaging GDPR-to-DPDP gap analysis under time pressure, three deltas warrant immediate architectural attention. First, the absence of legitimate interest as a lawful basis means many analytics, marketing, and fraud-prevention flows that currently rely on it must be re-architected around consent. Second, the under-18 threshold for children's data is four years higher than the most permissive GDPR standard and requires a verifiable parental consent mechanism most platforms do not currently operate. Third, the negative list approach to cross-border transfers is operationally inverted from GDPR's adequacy model — simpler in principle, but creates unpredictability when the Government notifies restrictions.

CHAPTER 04 · THE STANDARD

What valid consent actually looks like *under DPDP.*

Consent under DPDP is not a checkbox. It is a legal artifact with five mandatory properties, and the Data Fiduciary carries the burden of proving each one was satisfied at the moment of collection.

The Act sets out five elements. Each can fail independently. All five must be satisfied simultaneously for consent to be valid.

NO.	ELEMENT	WHAT IT MEANS IN PRACTICE
01	Free	The Principal must have a genuine choice. Consent bundled with essential service access — "agree to everything or you cannot proceed" — is not free.
02	Specific	Each distinct purpose requires its own consent. A single catch-all consent covering marketing, analytics, and partner sharing is not specific.
03	Informed	The notice accompanying consent must state what data, why, who processes it, and the rights available. Hiding processors in a linked policy does not satisfy this.
04	Unconditional	Consent to a purpose beyond what is strictly necessary cannot be a condition for service delivery. Pre-ticked boxes, or access gated on marketing opt-in, fail here.
05	Unambiguous	A clear affirmative action. Silence, pre-ticked checkboxes, or inferring consent from continued use of a service do not count.

Good vs bad consent, visualised

✗ FAILS STANDARD

Welcome to Acme

Create your account to continue

☑ I accept the Terms, Privacy Policy, and consent to marketing communications, analytics, and partner sharing.

Create Account

Pre-ticked by default. Bundled purposes.

*Fails **Specific** (bundled purposes), **Unambiguous** (pre-ticked), and **Free** (no granular choice).*

✓ MEETS STANDARD

Welcome to Acme

Required to create your account:

☐ **Account creation** — name, email, password. Full notice →

Optional:

☐ **Product updates** — monthly email, unsubscribe anytime.

☐ **Personalisation** — usage analytics to improve features.

Continue | Only essentials

Granular, unchecked, plain language. Optional purposes do not gate the service.

Checklist for product teams

- ☐ **One purpose, one consent.** Do not bundle marketing, analytics, and partner sharing under a single checkbox.
- ☐ **No pre-ticked boxes.** The Principal must affirmatively tick. Default-on is default-invalid.
- ☐ **Plain-language notice alongside, not behind a link.** If critical information requires a click-through, it is not informed consent.
- ☐ **Withdrawal as easy as grant.** The same number of clicks to withdraw as it took to consent.
- ☐ **22-language support** for the notice, or a clear language-selection mechanism before collection.
- ☐ **Timestamped consent record** — which purpose, which version of notice, which mechanism — retained for 7 years under the 2025 Rules.

CHAPTER 05 · THE COMPLEXITY

The operational complexity most enterprises *aren't prepared for.*

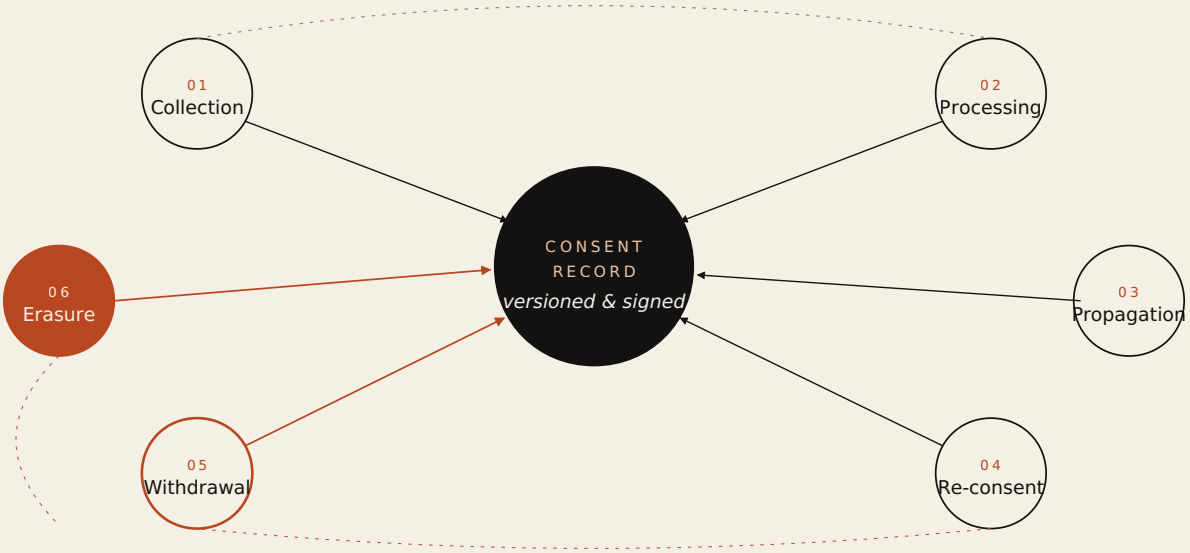
Consent collection is a design problem. Consent *management* — over the lifecycle of a Data Principal relationship — is an engineering problem at a scale most compliance programmes underestimate.

At the moment a user clicks "I consent," compliance leaders often treat the problem as solved. In practice, this is the point at which the harder problem begins. Consent must be versioned against the notice in effect at collection, propagated to every downstream processor, re-solicited when purposes change, withdrawable at any moment through any reasonable channel, and — on withdrawal — cascaded as deletion across every system that holds the record.

A consent record, in other words, is not a boolean in a database. It is a living object that changes state continuously across a distributed system.

FIGURE 01

The consent lifecycle



Each of the six states triggers obligations for the Data Fiduciary. Withdrawal (05) and Erasure (06) are the phases most commonly mishandled — often because systems were built with collection in mind and never planned for the reverse flow.

The 2025 Rules: specific timing obligations

The Digital Personal Data Protection Rules, 2025 translate the Act's abstract obligations into a governed data lifecycle with hard timing requirements. Four phases, each with distinct operational deliverables:

01
Phase

Ingestion

RULES 3, 4, 10

Standardised, accessible notices embedded across every channel of collection. Strict Consent Manager governance, entry criteria, and verifiable parental age-gating for minors.

02
Phase

Management

RULES 5, 6, 14

Auditable consent records with system-wide encryption, role-based access, and user-accessible mechanisms for exercising data rights.

7-YEAR CONSENT RETENTION

03
Phase

Incident & Resolution

RULES 7, 15

Mandated breach notification to the Data Protection Board and affected Principals. SLA-driven grievance workflows with documented escalation paths.

72-HR BREACH NOTIFICATION

90-DAY GRIEVANCE SLA

04
Phase

Sunset

RULE 8

Automated lifecycle tracking, verified erasure once purpose is fulfilled or consent withdrawn. Access and processing logs retained to support later audit.

1-YEAR LOG RETENTION PRE-ERASURE

The common failure points

Failure 01

Consent drift across versions

Notice changes over time, but the consent record is not versioned. When asked which notice a user consented to in 2024, the Fiduciary cannot produce it.

Failure 02

Orphaned processor sharing

Consent is withdrawn in the primary system, but the record was already sent to a downstream processor — CRM, ad network, warehouse — and never revoked there.

Failure 03

Children's data without verification

Self-declaration of age is not verifiable consent. Platforms that rely on "I am over 18" checkboxes have no defensible verification mechanism when challenged.

Failure 04

Asymmetric grant and withdrawal

Consent takes one click. Withdrawal requires an email, a customer-service call, and a 72-hour wait. The Act requires parity of effort.

Failure 05

Policy updates without re-consent

Privacy policy is updated to add a new processing purpose, but existing users are not re-prompted. Their original consent does not cover the new purpose.

Failure 06

Unprovable consent history

No immutable audit trail exists of who consented to what, when, and via which interface. In a Board inquiry, the Fiduciary cannot demonstrate the moment of collection.

> *A consent record is not a boolean. It is a living object that changes state continuously across a distributed system.*

CHAPTER 06 · THE FRAMEWORK

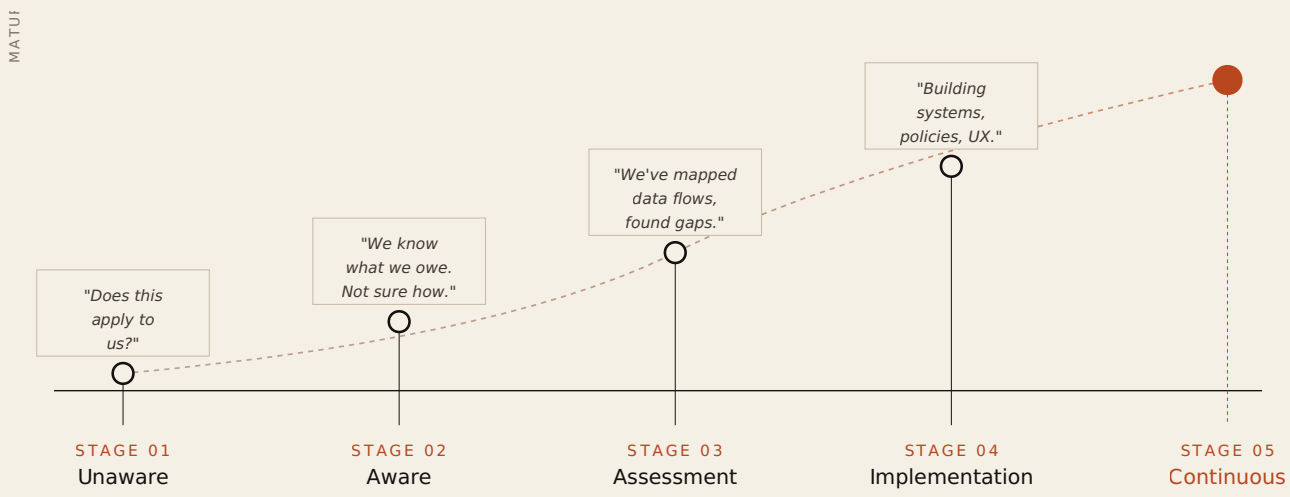
A practical DPDP readiness framework for *enterprises.*

Compliance maturity is not binary. The most effective programmes progress through five observable stages, each with its own set of questions, capabilities, and evidence.

Locating the organisation honestly on this curve is the first exercise. Most enterprises are in Stage 2 or early Stage 3 — aware of the obligations, mid-assessment, but not yet operationally ready. The framework below is diagnostic before it is prescriptive.

FIGURE 02

The five-stage DPDP readiness maturity model



Progression is not linear — enterprises can regress if policy is updated without re-engineering, or if an acquisition introduces a lower-maturity business unit. Most Indian enterprises today sit between Stage 02 and Stage 03.

What moves an organisation forward

STAGE	KEY CAPABILITY	ACTION TO ADVANCE TO NEXT STAGE
01	Unaware	Board-level briefing on DPDP scope and penalty exposure. Appoint a DPDP sponsor at Executive Committee level.

STAGE	KEY CAPABILITY	ACTION TO ADVANCE TO NEXT STAGE
02	Aware	Commission a formal scope assessment: which entities, which data, which jurisdictions. Establish a cross-functional DPDP working group.
03	Assessment	Complete data flow mapping, processor inventory, consent audit, and gap analysis. Produce a prioritised remediation roadmap with owners and timelines.
04	Implementation	Deploy consent management, update notices across products, re-consent existing user base where required, wire grievance workflows, establish breach response runbook.
05	Continuous	Quarterly audit cadence. DPIA pipeline for new products. Automated monitoring of consent drift and processor compliance. Regular Board reporting.

CHAPTER 07 · THE STACK

Technology requirements for DPDP compliance: *what your stack needs.*

DPDP compliance is a multi-layered architectural challenge, not a single software purchase. No standalone vendor category independently delivers full compliance — it requires a coordinated model across consent, lifecycle, data management, and security.

A defensible compliance stack has four functional layers. Each layer corresponds to an obligation or set of obligations. Each must be observable — because what cannot be shown to a regulator may as well not exist.

FIGURE 03

Reference architecture for a DPDP-compliant data processing stack

The framework deliberately mirrors the architectural model enterprises are adopting — policy & workflow at the top, user-facing consent orchestration at the core, data governance underneath, and security infrastructure at the foundation. Every transaction across these layers must produce an immutable record.

What each layer must deliver

LAYER	REQUIRED CAPABILITY
Advisory & Workflow	Interpret definitions and classify roles (Fiduciary vs Processor). Document legitimate uses and exemptions. Conduct continuous audits, DPIAs, and DPO oversight. Prepare for voluntary undertakings and Board engagement.
Consent Management (CMP)	Multilingual notice generation and delivery. Interoperable consent capture with granular purpose control. Immutable consent records with easy withdrawal. Accessible nomination and rights interfaces.
Data Management	Automated retention policies and deletion workflows. Accurate cross-border transfer mapping. Visibility over third-party processors. Data catalogue and lineage for every personal data element.
Infrastructure & Security	Encryption, tokenisation, and RBAC across all systems. 72-hour breach detection and response pipeline. Privacy-by-design embedded in product architecture.

IMPLEMENTATION · ZTRUST BY PRODEVANS

ZTrust delivers the compliance architecture as an integrated platform.

ZTrust is Prodevans' privacy and compliance platform, purpose-built for DPDP. It brings the four architectural layers into a single, observable operating system — so compliance teams stop stitching point tools together and start running a defensible programme. At its heart sits **Swikruti**, the consent management module that turns "I agree" into a verifiable, revocable, auditable artifact across every downstream system.

CORE

Swikruti

Consent orchestration, notice delivery, Data Principal portal, withdrawal and rights workflows.

DATA

Data Governance

Retention automation, processor tracking, cross-border mapping, cascading erasure.

EVIDENCE

Audit Trail

Immutable consent and processing records, grievance SLA monitoring, Board-ready reporting.

IN CLOSING

DPDP is not a *project.* It is a *posture.*

Every enterprise that processes personal data in India will arrive at continuous compliance eventually. The only variable is whether the path runs through a Board inquiry or through a deliberate programme.

The framework in this document — obligations, consent discipline, maturity, architecture — is the skeleton of that programme. The muscle is operational: the systems, the workflows, the evidence, the continuous loop between product, legal, and engineering that turns a written policy into a defensible posture on any day a regulator decides to ask.

PUBLISHER

PLATFORM

About Prodevans and ZTrust

Prodevans Technologies is a premier digital infrastructure and security solutions provider specializing in high-stakes regulatory compliance. Through its proprietary ZTrust suite, the firm delivers end-to-end identity governance and data privacy frameworks designed to ensure seamless organizational adherence to the DPDP Act 2023.

ZTrust is Prodevans' integrated DPDP compliance platform. It unifies consent management, data governance, and audit evidence into one operating layer — engineered specifically for the obligations of the Digital Personal Data Protection Act and its 2025 Rules.

Swikruti — from the Sanskrit word for consent — is the consent orchestration module at the core of ZTrust. It provides the notice delivery, Data Principal experience, withdrawal workflows, and immutable audit trail that turn consent from a checkbox into a provable, continuous operating discipline.

Ready to move your DPDP programme from assessment to implementation?

SPEAK TO OUR TEAM →