Operationalising India's DPDP Framework: An Analysis of the November 2025 DPDP Rules and Their Implications for AI-Driven Used-Car Marketplaces

Abstract

The Digital Personal Data Protection Act, 2023 (DPDP Act) and the Digital Personal Data Protection Rules, 2025 (DPDP Rules) together establish a comprehensive, principle-based regime for the processing of digital personal data in India. The notification of the DPDP Rules in November 2025 operationalises the Act by specifying procedures, timelines and detailed obligations relating to consent, security safeguards, breach notification, data retention and governance. This article undertakes a doctrinal and policy analysis of the DPDP framework with a particular focus on AI-driven digital platforms and used-car marketplaces. It asks how the Rules reshape data-driven business models that aggregate, enrich and algorithmically process consumer and vehicle-related data across multiple platforms.[1][2] [^3]

Using a mixed methodology combining black-letter analysis of the Act and Rules with a case-study of a representative used-car discovery platform, the article argues that the DPDP framework incentivises a shift from opaque data monetisation strategies toward purpose-specific, consent-anchored processing and demonstrable governance. It further contends that platforms positioning themselves as a "trust and intelligence layer" in the used-car ecosystem can translate compliance into a strategic differentiator by embedding privacy-preserving design, algorithmic transparency and ecosystem governance into their operating models.[2][4] [^5]

Keywords

Digital Personal Data Protection Act; DPDP Rules 2025; data protection; AI governance; used-car marketplaces; consent managers; algorithmic accountability; India.

1. Introduction

India's digital economy has experienced rapid expansion, with platform-mediated markets emerging in sectors as diverse as mobility, finance, retail and used vehicles. This growth has been accompanied by increasing volumes of personal data being processed, often in opaque ways and through complex multi-party ecosystems. The Digital Personal Data Protection Act, 2023 represents the culmination of a decade-long policy process to establish a dedicated legal framework for personal data protection.[6][7] [^1]

In November 2025, the Central Government notified the Digital Personal Data Protection Rules, 2025 pursuant to section 40 of the DPDP Act, thereby giving full operational effect to the statute. The Rules specify commencement timelines, define procedural and technical

obligations for Data Fiduciaries and processors, and elaborate mechanisms for consent management, security safeguards, breach reporting, retention and governance.[3][1]

This article examines the architecture and implications of the DPDP Rules from the perspective of AI-driven platforms, with a particular focus on used-car discovery and verification services that aggregate listings and behavioural data across multiple marketplaces. It poses three interrelated research questions:

1. How do the DPDP Rules operationalise the core principles and concepts of the DPDP Act?
2. What are the implications of the Rules for data-intensive, AI-enhanced platform business models in multi-party ecosystems?
3. How might an AI-driven used-car discovery platform adapt its governance, technical architecture and ecosystem contracts to align with the DPDP framework while preserving innovation capacity?

The analysis proceeds by first outlining the legal and policy background (Section 2), then describing the methodology (Section 3), before turning to the core features of the DPDP Rules (Section 4), their impact on data-intensive platforms (Section 5), and a case-study–based application to a used-car discovery platform (Section 6). Section 7 discusses broader theoretical and policy implications, and Section 8 concludes.

2. Regulatory background and policy context

2.1 Evolution of India's data protection regime

Prior to the enactment of the DPDP Act, personal data protection in India was primarily governed by the Information Technology Act, 2000 and its 2011 rules on sensitive personal data or information, supplemented by sectoral regulations in areas such as finance and telecommunications. These instruments were widely regarded as insufficient to address the scale, complexity and cross-border nature of contemporary data processing.[7][8]

The DPDP Act, enacted in August 2023, introduced a dedicated, principles-based framework governing the processing of digital personal data by both public and private entities. It created the concepts of "Data Fiduciary" (analogous to a data controller) and "Data Principal" (the individual to whom the data relates), established core processing principles and rights, and set up the Data Protection Board of India (DPB) as the enforcement authority. [1][7]

2.2 Objectives and design philosophy of the DPDP framework

Official communications portray the DPDP framework as "citizen-centric" and guided by the acronym SARAL: Simple, Accessible, Rational and Actionable. This design seeks to balance individual rights with innovation and ease of doing business by emphasising clear notices, meaningful consent, proportionate safeguards and accountable governance rather than prescriptive technical checklists.[2][3] [^1]

From a policy perspective, the DPDP framework reflects a convergence between global data protection trends—such as principles of purpose limitation, data minimisation, accuracy,

storage limitation and security safeguards—and India-specific concerns, including digital inclusion, State functions and start-up growth.[4][2]

3. Methodology

This article employs a mixed methodology combining doctrinal legal analysis with an applied case-study approach.

First, it undertakes black-letter analysis of the DPDP Act and the DPDP Rules, 2025, focusing on statutory text, official notifications and explanatory materials issued by the Government. This is complemented by a review of practitioner commentary and guidance from law firms, consulting organisations and dedicated privacy resources, which collectively interpret the Rules' implications for businesses.[9][3] [4][1] [^2]

Secondly, the article develops a case study of a representative AI-driven used-car discovery platform that aggregates listings and behavioural data across multiple marketplaces. Publicly available descriptions of such platforms' business models, data flows and positioning as a "trust and intelligence layer" in the used-car ecosystem are used to construct an illustrative scenario. The DPDP framework is then applied to this scenario to derive practical governance and design implications.[5][10]

This methodology is appropriate for at least two reasons. Doctrinal analysis permits careful exposition of statutory obligations and regulatory expectations, while the case-study approach bridges the gap between high-level legal norms and concrete implementation challenges for data-intensive platforms.[4][9]

4. The DPDP Rules, 2025: architecture and core features

4.1 Commencement and phased implementation

The DPDP Rules, 2025 were notified in mid-November 2025 and adopt a staggered commencement structure. Rules relating to commencement, definitions, governance and the functioning of the Data Protection Board entered into force immediately upon publication. Provisions concerning Consent Managers become effective one year after notification, while the remaining operational rules—including those governing privacy notices, security safeguards, breach notification, children's data, significant data fiduciaries and retention—take effect eighteen months after notification.[3][1] [2][4]

This three-phase schedule creates a compliance runway extending to approximately May 2027 for full operational obligations, with earlier phases focused on institutional set-up and ecosystem preparation.[9][2] [^4]

4.2 Structured privacy notices and consent

Rule-level elaboration of the DPDP Act's consent requirements mandates structured, standalone privacy notices that clearly identify categories of personal data collected, specific purposes of processing, and mechanisms for withdrawal of consent and exercise of rights.

Notices must be concise, written in clear language and distinct from general terms and conditions, in line with the SARAL design philosophy.[1][2] [3][4]

The Rules also operationalise the concept of "Consent Managers" introduced by the Act. These are independent, registered entities that provide interoperable platforms through which Data Principals can grant, manage and withdraw consent across multiple Data Fiduciaries. Eligibility criteria, governance requirements and obligations on record-keeping and security are specified, and Data Fiduciaries that integrate with Consent Managers must be capable of ingesting standardised consent artefacts and honouring revocations.[2][9]

4.3 Security safeguards and breach notification

The DPDP Rules require Data Fiduciaries to implement appropriate technical and organisational measures to ensure the security of personal data, including controls such as encryption, access management, logging, backup and continuity planning. Practitioner guidance emphasises that these measures are to be treated as baseline obligations rather than optional best practices.[3][4] [^9]

A dedicated breach-notification framework obliges Data Fiduciaries to inform both the Data Protection Board and affected Data Principals without undue delay upon becoming aware of a personal data breach. Initial intimation to the Board is expected promptly, followed by more detailed reporting within specified periods, and individuals must receive information about the nature of the breach, potential consequences and recommended mitigation steps.[4][9] [^3]

4.4 Retention, children's data and significant data fiduciaries

The Rules impose retention-management obligations, including conditions under which personal data may need to be erased after periods of user inactivity, subject to exceptions for legal or regulatory retention requirements. They also elaborate the Act's protections for children by requiring verifiable parental consent for processing children's personal data and restricting certain forms of profiling and targeted advertising.[2][4]

Additionally, the framework provides for the designation of "Significant Data Fiduciaries" (SDFs) based on factors such as volume and sensitivity of personal data processed, risk of harm, use of emerging technologies and impact on national interests. SDFs are subject to enhanced obligations, including data protection impact assessments (DPIAs), independent audits, appointment of a Data Protection Officer and, where specified, conditions on cross-border transfers.[7][4] [^2]

5. Implications for data-intensive digital platforms

5.1 Shifts in consent, purpose specification and data monetisation

The combined effect of structured privacy notices, consent-manager integration and retention limits is to disincentivise broad, bundled consent models and indefinite data reuse for unspecified monetisation strategies. Data Fiduciaries are encouraged to articulate specific, granular purposes for which personal data is processed, differentiate between core service delivery and optional value-added processing, and provide easy mechanisms for consent withdrawal.[4][2]

For data-intensive platforms, this entails unbundling uses such as personalised recommendations, cross-platform analytics, fraud detection, financing referrals and marketing communications, and aligning each use with a traceable lawful basis and auditable records.[9][4]

5.2 Accountability in multi-party ecosystems

The DPDP framework recognises complex data ecosystems involving Data Fiduciaries, processors, Consent Managers and State bodies, and places strong emphasis on contractual and governance arrangements that allocate responsibilities across the value chain. Commentators underscore the importance of Data Processing Agreements (DPAs), audit rights, security clauses and coordinated breach-notification cascades.[1][9] [2][4]

Platforms that integrate data from multiple sources—such as e-commerce aggregators, travel meta-search engines or used-car discovery services—must therefore map data flows end-to-end and determine, for each processing activity, whether they act as an independent Data Fiduciary, a processor or a joint controller, with corresponding duties in relation to notices, consent, rights handling and breach response.

5.3 Algorithmic transparency and AI governance

While the DPDP Act and Rules do not employ the term “artificial intelligence” extensively, obligations relating to accuracy, purpose limitation, DPIAs for SDFs and protections against digital harms collectively encourage more transparent and accountable use of algorithmic systems. Guidance for organisations suggests documenting data sources, feature engineering, model objectives and testing protocols, especially where algorithmic outputs influence access to services such as credit, insurance or employment.[7][9] [2][4]

This has particular salience for platforms that deploy machine-learning models for ranking, recommendation, trust scoring or fraud detection, where opaque algorithms can introduce bias or harm Data Principals if not subject to adequate governance and oversight.

6. Case study: an AI-driven used-car discovery platform

6.1 Business model and data ecosystem

Used-car marketplaces in India have evolved from classified listings to integrated platforms offering inspection, pricing, financing and warranty services. A newer class of platforms positions itself as a “trust and intelligence layer” that aggregates and verifies listings from multiple marketplaces, dealers and private sellers, providing cross-platform search, verification explainers and data-driven insights for buyers.[10][5][^6]

Publicly available descriptions indicate that such a platform aggregates listings, normalises attributes (for example, vehicle make, model, variant, mileage and price), overlays AI-based verification and market-context signals, and offers tools for users to compare options across platforms. User behaviour data—searches, filters, saved vehicles, feedback—and third-party signals—reviews, pricing trends, inspection results—are combined to generate recommendations and trust indicators.[^5]

6.2 Data flows and role classification under the DPDP framework

From a DPDP perspective, this business model involves several categories of personal data: user profile and contact information; usage and behavioural data; communication logs; and personal data embedded in listings and transaction histories (such as seller details, owner histories or location information).[6][10]

The platform is a Data Fiduciary in relation to users who interact directly with its services. Depending on contractual arrangements with upstream marketplaces and dealers, it may also act as:

- an independent Data Fiduciary when it determines purposes and means of processing listing data to create value-added services;
- a processor when it processes personal data solely on documented instructions of a marketplace or dealer; and
- a joint controller where purposes and decisions are jointly determined.

Accurate mapping of these roles is critical to designing compliant notice and consent mechanisms, allocating responsibilities for rights handling and breach notification, and drafting appropriate contractual provisions.[2][4]

6.3 Lawful bases, purpose limitation and retention

For user-facing processing, consent is likely to be the primary lawful basis for account creation, personalised recommendations, cross-platform search and marketing communications, complemented by legitimate uses recognised in the DPDP Act for fraud prevention, security and legal compliance. Privacy notices and consent interfaces should therefore distinguish between:[7][1]

- data strictly necessary for core service delivery (for example, processing search queries and displaying listings);
- optional data processing for enhanced experiences (alerts, saved searches, financing or insurance offers); and

- processing for security and fraud-detection.

Retention schedules must be defined by category, taking into account any inactivity-based deletion expectations articulated in the Rules and carving out exceptions for legal retention obligations. Technical capabilities for deletion or irreversible anonymisation must be implemented to operationalise these schedules.[4][2]

6.4 Security architecture and incident response

Given the sensitivity and volume of personal data processed, an AI-driven used-car discovery platform must implement security measures aligned with the DPDP Rules, including encryption, strong authentication, access controls, logging and monitoring. Security governance should encompass secure development practices for AI and recommendation engines, vulnerability management, change management and periodic independent assessments.[3][4]

An incident-response framework is required to detect, investigate and respond to personal data breaches. This must include procedures for timely notification to the Data Protection Board and affected individuals, documentation of incidents and remedial steps, and integration with partner platforms where breaches implicate shared data.

6.5 AI lifecycle management and trust-scoring governance

Because the platform's competitive advantage derives from AI-based verification and trust scoring, DPDP-aligned AI governance becomes central. Recommended practices include documenting model-development pipelines, testing for bias and disparate impact where models influence rankings or recommendations, and constraining the use of personal data in training to purposes consistent with original collection or with fresh consent where required. [9][4]

User-facing explanations of trust scores and verification labels should be provided in accessible language, clarifying what these indicators signify and on what broad factors they are based. This supports both transparency norms and the platform's positioning as a trusted intermediary.

7. Discussion: DPDP compliance as strategic governance

The application of the DPDP framework to AI-driven used-car platforms illustrates how compliance can be framed not merely as a regulatory burden but as an opportunity to strengthen governance, user trust and ecosystem relationships. By integrating DPDP principles into product design, data architecture and partnership contracts, platforms can create "privacy-by-design" and "accountability-by-design" capabilities.[9][4]

Proactive readiness for potential Significant Data Fiduciary designation—through early adoption of DPIA methodologies, independent audits and algorithmic accountability practices—can also enhance resilience and attractiveness to regulated partners such as banks and insurers. Conversely, neglecting DPDP obligations risks not only regulatory sanctions but also reputational damage in a market where trust is a key differentiator.[7][2]

8. Conclusion

The November 2025 notification of the DPDP Rules, 2025 represents a pivotal moment in the evolution of India's data protection regime, transforming the DPDP Act's high-level principles into concrete, enforceable obligations for entities processing digital personal data. For AI-driven used-car discovery platforms and similar data-intensive businesses, the framework necessitates re-examination of consent models, data flows, security architectures, algorithmic governance and ecosystem contracts.[1][3]

This article has argued that such platforms can respond to the DPDP framework not merely by seeking minimal compliance but by embedding privacy, transparency and accountability into their core value propositions. Doing so can simultaneously meet regulatory expectations, mitigate risk and enhance competitive positioning in India's rapidly evolving digital mobility economy.[5][4]

References

1. DPDP Rules, 2025 Notified
2. India's DPDP Rules Are Now Notified: What Actually Changes for ... - On 13 November 2025, the Government officially notified the Digital Personal Data Protection Rules, ...
3. 620 Used Cars in Odisha - Second Hand Cars for Sale with EMI ... - Browse from over 620 thoroughly inspected, pre-owned cars in Odisha , with prices starting at just ₹...
4. DPDP Rules, 2025 Notified - पत्र सूचना कार्यालय - Press Information Bureau (PIB) is the nodal agency of the Government of India to disseminate informa...
5. DPDP Compliance in 2025: What Every Business Must Do Under ... - DPDP Compliance in 2025: What Every Business Must Do Under the Latest November Rules · 1. Data Mappi...
6. CarArth - Find Your Car. Trust the Search. - CarArth is India's trust and AI intelligence layer for used-car discovery. It verifies listings from...
7. DPDP Rules 2025: Understand India's Data Protection Laws - Lawrbit - Explore DPDP Rules 2025 and key updates under the Digital Personal Data Protection Act 2023. Learn c...
8. [PDF] DPDP Act + Rules 2025: Effective Sections, Deadlines and What To ... - The notification brings DPDP Rules, 2025 into force in ... The 13 November 2025 notification activat...
9. Which Used Car Platform Is Actually Best for Buyers in India ... - Discover which used car platform is best for your needs in India. We compare Cars24, Spinny, CarWale...
10. Data protection laws in India