The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

UNDERSTANDING THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023:

KEY COMPLIANCE REQUIREMENTS FOR BUSINESSES

~AFNAN MUNAF QURESHI

ABSTRACT

India's Digital Personal Data Protection Act, 2023("DPDP Act" or "the Act")1 marks the result of a long process of data protection laws. This began with the Supreme Court's recognition of privacy as a fundamental right and the recommendation made by Justice B.N. Srikrishna Committee2. The Act has now become fully operative with the notification of the Digital Personal Data Protection Rules, 2025 and the establishment of the Data Protection Board of India.

This article examines the compliance architecture the DPDP Act creates for businesses acting as Data Fiduciaries: the grounds for lawful processing and consent, core duties such as data minimization, security safeguards and breach notification, the retention and erasure of data, grievance redressal, and the enhanced obligations imposed on Significant Data Fiduciaries.

It further considers the rights conferred on Data Principals, the practical challenges of implementation for start-ups, mid-sized enterprises and multinational entities, and situates the Indian framework within a comparative perspective alongside the European Union's General Data Protection Regulation. The article concludes that while the DPDP Act adopts a deliberately simple and principle-based drafting style, its true compliance burden will be defined by subordinate rule-making and the enforcement practice of the Data Protection Board, making proactive, audit-ready compliance programs indispensable for Indian and foreign businesses alike.

[1] Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).

[2] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).

Keywords: DPDP Act 2023; Digital Personal Data Protection Rules, 2025; Data Fiduciary; Data Principal; Consent Manager; data breach notification; cross-border data transfer; Data Protection Board of India; GDPR comparison; privacy compliance.

INTRODUCCTION

Personal data has become the principal raw material of the digital economy. Every transaction, subscription, loan application, ride booked or prescription filled leaves a trail of digital personal data that is collected, stored, analyzed and, frequently, monetized by the entities that gather it. As India's digital economy has expanded to encompass well over 800 million internet users, the absence of a dedicated statutory framework for the protection of such data had, for over two decades, been addressed only indirectly, through sectoral rules under the Information Technology Act, 2000 and its subordinate rules. The constitutional foundation for a comprehensive privacy law was laid in 2017, when a nine-judge bench of the Supreme Court of India held that the right to privacy, including informational privacy, is intrinsic to the right to life and personal liberty under Article 21 of the Constitution.

That judgment directed the Union Government to examine and put in place a data protection framework, a task subsequently undertaken by the Committee of Experts chaired by Justice B.N. Srikrishna, whose 2018 report formed the template for successive legislative drafts.

After multiple iterations, the Digital Personal Data Protection Bill, 2023 was passed by both Houses of Parliament and received Presidential assent on 11 August 2023, thereby enacting the DPDP Act. Substantial portions of the Act, together with the Digital Personal Data Protection Rules, 2025, were finally brought into force on 13 November 2025[3], operationalizing India's first standalone, cross-sectoral data protection law. This article examines the compliance obligations that the Act places on businesses functioning as Data Fiduciaries, the corresponding rights it confers on individuals as Data Principals, and the practical and doctrinal questions that the new regime raises. The discussion is organized to serve both an academic and a practitioner

[3] Comm. of Experts Under the Chairmanship of Justice B.N. Srikrishna, Ministry of Elecs. & Info. Tech., Gov't of India, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (2018).

readership: it explains the statutory architecture, distils the core compliance requirements into an operational checklist, and critically evaluates the Act's strengths and gaps in a comparative light.

OVERVIEW OF THE DPDP ACT, 2023

A. Background and Legislative Development

The DPDP Act represents the fourth legislative iteration of India's data protection project, following the Personal Data Protection Bill, 2018, the Personal Data Protection Bill, 2019, and the Data Protection Bill, 2021 reported by a Joint Parliamentary Committee. Each successive draft progressively diluted more onerous features of earlier versions, most notably the mandatory data-localization requirements proposed in 2018, in favor of a lighter-touch, principle-based statute. The final Act is deliberately drafted in plain language, following what the Government has described as a "SARAL" (simple, accessible, rational and actionable) approach, and rests on the identifiable principles of consent and transparency, purpose limitation, data minimization, accuracy, storage limitation, security safeguards, and accountability[4].

B. Key Definitions

The Act's obligations turn on a small set of defined actors and objects[5]. Personal data is any data about an individual who is identifiable by or in relation to such data. A Data Principal is the individual to whom the personal data relates — and, in the case of a child, includes the parent or lawful guardian, and, for a person with a disability, the lawful guardian. A Data Fiduciary is any person who, alone or with others, determines the purpose and means of processing personal data, and thus bears the primary compliance burden under the Act. A Data Processor processes personal data on behalf of a Data Fiduciary, typically under contract, but does not thereby escape the Fiduciary's overarching accountability. Finally, a Consent Manager is a novel intermediary, registered with the Data Protection Board of India, that provides Data

[4] Press Information Bureau, Government of India, "DPDP Rules, 2025 Notified" (13 November 2025), available at pib.gov.in.

[5] DPDP Act, 2023, s 2(t) read with s 2(h) (definitions of 'personal data' and 'data fiduciary'); s 2(j) ('Data Principal'); s 2(k) ('Data Processor').

Principals a single, interoperable interface through which to give, manage, review and withdraw consent across multiple Data Fiduciaries[6].

C. Key Compliance Requirements for Businesses

The heart of the DPDP Act, from a business perspective, lies in Chapter II, which sets out the obligations of Data Fiduciaries. These obligations can be organized into seven operational clusters.

1. Lawful Processing and Consent

A Data Fiduciary may process personal data only for a lawful purpose for which the Data Principal has given consent, or for specified "legitimate uses" enumerated in the Act (such as voluntary provision of data by the principal, medical emergencies, or compliance with law)[7]. Consent must be free, specific, informed, unconditional and unambiguous, indicated through clear affirmative action, and must relate only to the personal data necessary for the specified purpose. Every request for consent must be accompanied by an itemized notice, in English or any language listed in the Eighth Schedule to the Constitution, describing the personal data sought and the purpose of processing. Critically, a Data Principal may withdraw consent at any time with an ease at least comparable to that with which it was given, and withdrawal does not affect the lawfulness of processing carried out before it.

2. Duties of Data Fiduciaries

Beyond consent, Data Fiduciaries must process personal data only for the purpose for which consent was given or a permitted legitimate use, must take reasonable steps to ensure the accuracy and completeness of data used for decisions affecting a Data Principal or shared with another Fiduciary, and must observe data minimization, collecting no more personal data than is necessary for the stated purpose[8]. The obligation of purpose limitation is complemented by an accountability principle, under which the Data Fiduciary remains responsible for compliance irrespective of any contractual arrangement with a Data Processor.

3. Security Safeguards

Section 8(5) of the Act requires Data Fiduciaries to implement "appropriate technical and organizational measures" to ensure compliance and to prevent personal data breaches. The 2025 Rules give this obligation operational content, prescribing measures such as encryption

[6] DPDP Act, 2023, s 2(g)
[7] DPDP Act, 2023, ss 4–6
[8] DPDP Act, 2023, s 8

or masking of data, access controls, monitoring and logging to detect unauthorised access, business continuity and disaster-recovery arrangements, contractual security obligations flowing down to Data Processors, and retention of logs for a minimum of one year[9].

4. Data Breach Notification

Where a personal data breach occurs, the Data Fiduciary must intimate the Data Protection Board of India and every affected Data Principal[10], notifying without delay and furnishing a detailed report to the Board within seventy-two hours of becoming aware of the breach. Notably, the Act contains no materiality or de-minimis threshold: unlike the risk-based approach under the GDPR, every breach, however minor, must be notified to the Board and to affected individuals. This is among the more stringent features of the Indian regime and requires businesses to build breach-detection and reporting capability well in advance of any incident, rather than relying on after-the-fact remediation.

5. Retention and Deletion of Data

Consistent with the storage-limitation principle, a Data Fiduciary must erase personal data upon withdrawal of consent by the Data Principal, or as soon as it is reasonable to assume that the specified purpose is no longer being served, unless retention is necessary for compliance with any law[11]. Corresponding obligations require Data Processors to erase data on the instructions of the Fiduciary.

6. Grievance Redressal Mechanism

Every Data Fiduciary must establish an effective mechanism to redress the grievances of Data Principals, and must publish the business contact information of a person able to answer questions about the processing of personal data[12]. Where a grievance is not resolved satisfactorily, a Data Principal may complain to the Data Protection Board of India, which has been constituted with civil-court-like powers of inquiry and can impose the substantial monetary penalties prescribed under the Schedule to the Act.

7. Additional Obligations of Significant Data Fiduciaries

The Central Government may notify certain Data Fiduciaries as “Significant Data Fiduciaries” (SDFs), having regard to factors such as the volume and sensitivity of personal data processed,

[9] DPDP Act, 2023, s 8(5); DPDP Rules, 2025, r 6
[10] DPDP Act, 2023, s 8(6); DPDP Rules, 2025, r 7
[11] DPDP Act, 2023, s 8(7)–(8)
[12] DPDP Act, 2023, s 13

the risk to the rights of Data Principals, and considerations of electoral democracy, security of the State, and public order. SDFs face enhanced obligations: appointment of a Data Protection Officer based in India, appointment of an independent data auditor, and periodic Data Protection Impact Assessments and compliance audits[13]. These heightened duties mirror, in a more compact form, the accountability obligations placed on large-scale processors under comparable foreign regimes.

RIGHTS OF DATA PRINCIPALS AND THEIR IMPACT ON BUSINESSES

Correlative to the duties above, the Act confers a compact set of rights on Data Principals: the right to obtain a summary of personal data being processed and the identity of Data Fiduciaries and Processors with whom it has been shared; the right to correction, completion, updating and erasure of personal data; the right to a readily available means of grievance redressal; and the right to nominate another individual to exercise these rights in the event of death or incapacity[14]. For businesses, these rights translate into concrete operational demands: they must build verifiable identity-and-request-handling workflows, maintain data lineage sufficient to answer access requests accurately, and design consent and preference interfaces increasingly, in cooperation with registered Consent Managers that make withdrawal of consent no more cumbersome than its grant. The cumulative effect is to shift data governance from a peripheral legal function to a cross-departmental operational discipline touching product design, customer service, information security and vendor management alike.

CHALLENGES IN IMPLEMENTATION

Notwithstanding its concise drafting, the DPDP Act poses substantial implementation challenges. First, compliance costs — consent-management infrastructure, breach-detection tooling, data-mapping exercises and, for SDFs, dedicated compliance personnel — fall disproportionately on start-ups and small and medium enterprises with limited compliance budgets, even though the Rules provide a staggered, roughly eighteen-month implementation

[13] DPDP Act, 2023, ss 9–10
[14] DPDP Act, 2023, s 11

timeline intended to ease this transition[15]. Second, while Section 16 permits cross-border transfer of personal data to any jurisdiction not specifically restricted by the Central Government[16], the absence, as yet, of any notified restricted-country list, combined with sector-specific data-localizations mandates in areas such as payments regulation, leaves multinational businesses navigating a degree of residual uncertainty about which stricter sectoral rule prevails[17]. Third, cybersecurity preparedness remains uneven across sectors, and the 72-hour breach-notification clock, described above, exposes Data Fiduciaries with immature incident-response capability to considerable penalty risk. Finally, several operational questions the precise criteria for designating Significant Data Fiduciaries, the detailed procedure before the Data Protection Board, and the interaction between DPDP breach-notification duties and pre-existing CERT-In reporting obligations under the Information Technology Act — continue to depend on further regulatory clarification and evolving Board practice[18].

COMPARATIVE PERSPECTIVE

A comparison with the European Union's General Data Protection Regulation[19] is instructive. Both frameworks share a consent-and-accountability architecture and comparable principles of purpose limitation and data minimization. They diverge, however, in significant respects. On cross-border transfers, the GDPR operates a restrictive “whitelist” model, prohibiting transfer outside the European Economic Area absent an adequacy decision or an approved safeguard mechanism such as standard contractual clauses; the DPDP Act inverts this logic into a permissive “blacklist” model, allowing transfer to any jurisdiction except those the Central Government specifically restricts. On breach notification, the GDPR conditions notification of individual data subjects on a risk-based threshold, whereas the DPDP Act requires notification of every breach to every affected Data Principal, without exception. The DPDP Act also omits

[15] See DPDP Rules, 2025, Second Schedule (staggered, roughly eighteen-month compliance timeline for various categories of obligations); Press Information Bureau (n 5) (noting that 6,915 stakeholder inputs, including from start-ups, MSMEs, industry bodies and civil society, were received during the consultation on the draft Rules held across seven Indian cities).

[16] DPDP Act, 2023, s 16

[17] Lexology, "India’s Digital Data Protection Act 2023: Key Insights and Comparisons with GDPR" (5 March 2025).

[18] EY India, "DPDP Act 2023 and DPDP Rules 2025: Compliance Guide" (December 2025).

[19] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation) [2016] OJ L119/1, arts 44–49 (adequacy decisions and transfer safeguards).

several GDPR features altogether — there is no free-standing "right to data portability" and no explicit "right to be forgotten" distinct from the erasure obligation tied to consent withdrawal while introducing the Consent Manager, an intermediary institution without a direct GDPR analogue. These differences reflect a deliberate legislative choice to priorities ease of compliance and innovation-friendliness over the GDPR's more prescriptive, rights-maximizing model.

CRITICAL ANALYSIS

The DPDP Act's central achievement is to finally give India a horizontally applicable data protection statute, replacing a patchwork of sectoral and contractual protections with an enforceable set of rights and obligations, backed by a dedicated regulator in the Data Protection Board of India. It's plain-language drafting and phased, roughly eighteen-month compliance runway are genuine strengths for a jurisdiction with as heterogeneous a business base as India's. The steep penalties available under the Schedule to the Act up to ₹250 crore for security-safeguard failures and up to ₹200 crore for breach-notification failures signal that the Government intends the regime to have real deterrent force[20].

Yet the Act's brevity is also, in places, a source of ambiguity. Several exemptions including a broad carve-out for processing by the State and its instrumentalities in the interests of sovereignty, security and public order, and a consequential narrowing of the right to information under Section 8(1)(j) of the Right to Information Act, 2005[21] have attracted criticism for potentially privileging governmental processing over the citizen-facing transparency the Act otherwise promotes. The absence of an independent adjudicatory tribunal, with the Data Protection Board instead constituted by the Executive, has similarly drawn commentary questioning the Board's institutional independence.

Finally, because so much operative detail the contours of "significant" data fiduciary status, the specifics of cross-border restrictions, and the practical scope of "legitimate use" exemptions has been left to delegated rule-making and evolving Board practice, the real compliance burden

[20] Schedule to the DPDP Act, 2023, read with s 33 (penalties of up to ₹250 crore for failure to implement reasonable security safeguards; up to ₹200 crore for failure to notify a breach; up to ₹200 crore for non-compliance with provisions on children's data; up to ₹150 crore for breach of Significant Data Fiduciary obligations; and up to ₹10,000 for breach of a Data Principal's duties).

[21] DPDP Act, 2023, s 44

on business will only become fully clear as the Rules are applied and interpreted over the coming implementation period.

CONCLUSION

The DPDP Act, 2023, together with the Digital Personal Data Protection Rules, 2025, establishes India's first comprehensive framework for the protection of digital personal data, translating the constitutional guarantee recognized in Puttaswamy into an enforceable statutory regime. For businesses, the Act's compliance requirements lawful processing and consent, purpose limitation and data minimization, security safeguards, mandatory breach notification, storage limitation, grievance redressal, and enhanced obligations for Significant Data Fiduciaries — collectively demand a shift from reactive, incident-driven privacy practice toward proactive, audit-ready data governance. As the phased implementation timeline runs its course through November 2026 and May 2027, and as the Data Protection Board of India develops its enforcement practice, businesses that treat DPDP compliance as an ongoing governance discipline rather than a one-time documentation exercise will be best placed to manage both regulatory risk and the reputational expectations of an increasingly privacy-conscious Indian digital economy.

References

- Statutes and Rules: Digital Personal Data Protection Act, 2023, No. 22 of 2023 (India); Digital Personal Data Protection Rules, 2025; Information Technology Act, 2000; Right to Information Act, 2005; Regulation (EU) 2016/679 (General Data Protection Regulation).
- Cases: Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
- Reports: Ministry of Electronics and Information Technology, Report of the Committee of Experts under the Chairmanship of Justice B.N. Srikrishna (2018).
- Secondary Sources: Press Information Bureau, Government of India (13 November 2025); EY India, DPDP Act 2023 and DPDP Rules 2025: Compliance Guide (December 2025); Lexology, India’s Digital Data Protection Act 2023: Key Insights and Comparisons with GDPR (5 March 2025); and further practitioner commentary as cited in the footnotes above.