BETWEEN TEXT AND TECHNOLOGY: UNPACKING THE HIDDEN BARRIERS TO DPDP COMPLIANCE

Gurveer Singh Dhindsa, LL.B. (Hons.), O.P. Jindal Global University,
Jindal Global Law School (2023-2026)

ABSTRACT

The Digital Personal Data Protection Act, 2023 ("DPDP Act")[1] and the Digital Personal Data Protection Rules, 2025 ("DPDP Rules")[2] together form India's first comprehensive, cross-sectoral data protection framework, enacted in fulfilment of the constitutional guarantee of privacy recognised in Justice K.S. Puttaswamy (Retd.) v Union of India.[3] While the framework promises clarity and informational self-determination, a close reading of its text reveals structural ambiguities that threaten its fidelity in practice. This paper examines five interlocking gaps: first, the confinement of "Data Principal" status to natural persons, leaving corporate and institutional personal data inadequately addressed; second, the disproportionate compliance burden that "verifiable parental consent" under Section 9 imposes on start-ups, absent graded obligations or regulatory sandboxes; third, the breadth of the State-exemption power under Section 17, tested against the necessity-and-proportionality standard in Puttaswamy; fourth, the risk that "certain legitimate uses" under Section 7[4] dilute the Act's affirmative-consent architecture into one of implied consent; and fifth, the contraction of Data Principal rights - notably data portability and the right to be forgotten - relative to the recommendations of the Justice B.N. Srikrishna Committee (2018) and the Joint Parliamentary Committee (2021).[5] The paper further considers the absence of a "sensitive personal data" category and the resulting friction with sectoral regulators such as the Reserve Bank of India, SEBI, and IRDAI, with reference to health and financial data. Drawing on the statutory text, pending litigation, parliamentary history, and scholarly commentary, the paper concludes that the DPDP regime requires interpretive discipline, judicial clarification, and targeted reform to fulfil the rights-protective promise of the Constitution and the Act's preamble.

[1]Digital Personal Data Protection Act 2023.
[2]Digital Personal Data Protection Rules 2025.
[3]*Justice K.S. Puttaswamy (Retd) v Union of India (2017) 10 SCC 1*.
[4]Digital Personal Data Protection Act 2023, s 7.
[5]Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (Government of India, 2018).

Research Questions

This paper is structured around six research questions. First, does the requirement under Section 2(k)[6] that a Data Principal be a natural person create a structural shortfall in the protection of personal data relevant to business and institutional settings, given the dual role companies occupy as Data Fiduciaries and, practically, as sources of personal data? Second, does the "verifiable parental consent" requirement under Section 9,[7] as elaborated in the DPDP Rules, 2025, impose disproportionate compliance burdens on start-ups and SMEs, and does the absence of graduated requirements, regulatory sandboxes, or financial support undermine the Act's stated aim of fostering a digital economy? Third, does the State-exemption power under Section 17 satisfy the necessity-and-proportionality test in Puttaswamy, and what is the significance of the pending constitutional challenge to Section 17? Fourth, is the concept of "certain legitimate uses" under Section 7,[8] particularly Section 7(a), sufficiently well-defined, or does it risk becoming a route through which the Act's affirmative-consent regime is displaced by a "slippery slope" of implied consent? Fifth, how does the rights framework under the DPDP Act, 2023 compare with the recommendations of the 2018 Committee of Experts[9] and the 2021 Joint Parliamentary Committee, and what are the normative implications of the absence of rights such as data portability and the right to be forgotten? Sixth, does the absence of a "sensitive personal data" category, combined with the overlapping jurisdiction of sectoral regulators such as the Reserve Bank of India, IRDAI, and SEBI, create regulatory uncertainty in areas such as health and finance?

I. Constitutional Promise to Statutory Text

The enactment of the Digital Personal Data Protection Act, 2023 and the notification of the Digital Personal Data Protection Rules, 2025 on 13-14 November 2025 mark the culmination of a long process that began with the Supreme Court's recognition of privacy as an inseparable part of the right to life and personal liberty in Puttaswamy. The preamble of the DPDP Act places this constitutional turning point at the heart of the legislation, stating that it seeks to balance the right of individuals to protect their personal data with the need to process such data for lawful purposes. It is this balance between protection and the facilitation of lawful

[6]Digital Personal Data Protection Act 2023, s 2(k).
[7]Digital Personal Data Protection Act 2023, s 9.
[8]Digital Personal Data Protection Act 2023, s 7.
[9]Committee of Experts under the Chairmanship of Justice B.N. Srikrishna (n 5).

processing - including by the State and by commercial actors - that forms the central tension of the Act, and it is this tension that the paper seeks to illuminate.

The DPDP Act, on its own terms, offers a simple, principle-based, and modern framework to replace India's earlier data-protection regime, which was cumbersome and rooted in Section 43A of the Information Technology Act, 2000[10] and the Sensitive Personal Data or Information Rules, 2011.[11] Yet the open texture of the Act, its structure of delegation, and the manner in which the 2025 Rules have filled the Act's gaps together create practical and doctrinal challenges that are not always apparent from the language of the Act alone. This paper takes the view that these are not surface-level flaws but structural traits that bear directly on the possibility of compliance, the internal coherence of the statute, and the extent to which the regime reflects the constitutional vision set out in Puttaswamy.

II. Constitutional Foundations: Puttaswamy and the Unfinished Promise of Informational Privacy

The constitutional judgment that made the DPDP Act possible - indeed, necessary - must be the starting point for any examination of the Act. A nine-judge bench of the Supreme Court in Puttaswamy held that the right to privacy forms part of the right to life and personal liberty under Article 21[12] and extends to informational privacy, understood as an individual's right to control the dissemination of personal information. Crucially, the Court did not treat privacy as an absolute right, but held that restrictions upon it, whether imposed by the State or otherwise, must satisfy a three-part test of legality (the existence of a law authorising the restriction), necessity (that the restriction serve a legitimate State aim), and proportionality (that the restriction be proportionate to that aim, with adequate procedural safeguards against abuse).

The DPDP Act's preamble can be read as an attempt to translate these constitutional principles into statutory form, stating that the Act recognises “the right of individuals to protect their personal data and the need to process personal data for lawful purposes.” On one reading, this restates the proportionality calculus contemplated in Puttaswamy - individual rights are recognised but may yield to legitimate countervailing interests, provided that such yielding is

[10]Information Technology Act 2000, s 43A.
[11]Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.
[12]Constitution of India, art 21.

grounded in law.[13] The central difficulty explored in this paper is signalled already in the preamble: the individual's right is framed narrowly and conditionally, while the countervailing State or commercial interest is framed broadly and is largely self-executing. Whether this asymmetry is constitutionally tolerable is a question to which this paper returns in examining the Section 17[14] exemptions and the Section 7[15] legitimate uses against the necessity-and-proportionality standard in Puttaswamy. The remainder of this paper traces the definitional and structural choices made in the DPDP Act, 2023 and the DPDP Rules, 2025 that flow from this constitutional inheritance.

III. Unpacking the Definitional Conundrum: "Data Principal" and the Exclusion of Juristic Persons

The definition itself is straightforward: only natural persons - or, in the case of a child, the parent or lawful guardian, and in the case of a person with disability, the lawful guardian - may be "Data Principals." This deliberate narrowing to "the individual" excludes companies, partnerships, trusts, and other juristic persons from the definition, and consequently from the substantive rights conferred by Chapter III, including the rights to information regarding processing, correction, erasure, and grievance redressal. The DPDP Act is not unusual in this respect: the GDPR's concept of "data subject" is likewise confined to natural persons, and India's choice broadly follows international practice.[16] The difficulty, therefore, is not that the DPDP Act departs from the global model, but that following that model produces consequences for India's data environment that the Act does not explicitly address - companies are forced to occupy a dual role as both fiduciaries and, de facto, as sources of personal data.[17]

Consider, for instance, a small business that uses a bank to open a current account on behalf of its directors, signatories, or key managerial personnel, or that uses a payment aggregator to onboard its directors, or that enters into a commercial contract through a vendor, thereby sharing the personal data of each with these entities. In each such relationship, the enterprise is, formally, merely a conduit through which the personal data of identified natural persons (its

[13]Gautam Bhatia, 'State Surveillance and the Right to Privacy in India: A Constitutional Biography' (2014) 26(2) National Law School of India Review 127.
[14]Digital Personal Data Protection Act 2023, s 17.
[15]Digital Personal Data Protection Act 2023, s 7.
[16]Apar Gupta and Ujwala Uppaluri, 'Privacy after Puttaswamy' (2018) 53(51) Economic and Political Weekly 45.
[17]Graham Greenleaf, 'India's Digital Personal Data Protection Act 2023: A Comparative Analysis' (2024) 187 Privacy Laws & Business International Report 1.

officers) flows to another Data Fiduciary; the enterprise, being a juristic person, cannot invoke the access, correction, or erasure rights under Sections 11 to 13 in respect of that data. Yet it is the enterprise that is more likely to bear the commercial consequences of any misuse, retention, or disclosure of that data - for instance, where a counterparty's mishandling of a promoter's personal data carries reputational or contractual consequences for the enterprise as a whole.

This gap is compounded by the fact that, in many small Indian businesses - proprietorships and partnerships in particular - the "personal data" of the proprietor or partners is functionally indistinguishable from the "business data" of the enterprise.[18] For most practical purposes, information about the business - its name, address, contact details, financial data - is simultaneously personal information of its owner. Because the DPDP Act confines its scope to natural persons, it leaves unanswered which of two regulatory approaches applies: is the proprietor a Data Principal entitled to the full suite of Chapter III rights (meaning that every commercial counterparty dealing with the proprietorship becomes subject to Data Principal rights claims that would not arise if the same business were incorporated)? Or does such data fall outside the Act's protective threshold altogether, as "business" rather than "personal" data? Neither the Act nor the 2025 Rules offer explicit guidance, leaving an interpretive void at the intersection of two areas central to India's economy: its vast informal and micro-enterprise sector, and the formal data-protection regime.

A further consequence of the narrow definition is that "corporate personal data" - data relating to employees, contractors, vendor representatives, and customer contact persons - is processed solely within an individual-centred framework, with no institutional mechanism through which the enterprise that is the true "owner" of the commercial relationship can assert an interest in how that data is used.[19] For instance, where a vendor's contract has ended and a counterparty continues to process the vendor's personnel data for a purpose unrelated to the original contract, only the individuals concerned - who may be wholly unaware that their data continues to be processed, let alone realistically positioned to invoke the Act's grievance mechanisms - have any basis for objection. The vendor enterprise itself has no corresponding interest it can assert in the protection of information contained in its personnel records, notwithstanding that such information may be misused by a former counterparty.

[18] Apar Gupta and Ujwala Uppaluri (n 16).
[19] Abhishek Singh and Anushka, 'The Digital Personal Data Protection, 2023: An Ambitious Government Step Towards Ensuring its Wide Reach' (2024) 70(3) Indian Journal of Public Administration 445.

It bears emphasis that the appropriate remedy for this deficit is not to extend "Data Principal" status to juristic persons - a step that would represent a radical departure from the GDPR model and from the recommendations of India's own expert committees, and that would risk eroding the emphasis on individual rights that is among the Act's central achievements. What is required, instead, is that the Data Protection Board of India, through its guidance, and the Central Government, through future amendments to the Rules, clarify how "corporate personal data" is to be treated in business-to-business settings - including by reference to contractual provisions under the Indian Contract Act, 1872 - and provide sector-specific guidance for proprietorships and partnerships regarding legitimate interests, in a manner that does not distort the core meaning of "Data Principal."[20]

IV. Verifiable Parental Consent: The Rule and the Compliance Burden

Section 9 of the DPDP Act[21] prohibits any processing of children's personal data that is not conducted in accordance with verifiable parental or guardian consent, and separately prohibits processing likely to cause detrimental effects on the well-being of a child, as well as tracking, behavioural monitoring, and targeted advertising directed at children. The Act defines "child" by reference to an age threshold higher than the "digital consent" age (typically thirteen or sixteen) adopted in many other jurisdictions, thereby bringing within the scope of "verifiable parental consent" a class of older adolescents who, in many other contexts, are treated as capable of making their own decisions.

The mechanism for obtaining "verifiable consent" is not specified in the Act itself but is left to delegated legislation. Under the DPDP Rules, 2025, two principal routes emerge. The first permits a Data Fiduciary to rely on an account already authenticated on its platform by a parent. The second - of far greater practical consequence for new entrants and new platforms - requires verification of identity and age either through a Digital Locker service or other authorised entity, or through a virtual token generated from identity and age information voluntarily furnished by the parent.[22] Data Fiduciaries must accordingly design, build, test, and maintain identity-verification pipelines, integrate with third-party identity infrastructure such as DigiLocker, and develop audit trails capable of withstanding the scrutiny of the Data

[20]Apar Gupta and Ujwala Uppaluri (n 16).
[21]Digital Personal Data Protection Act 2023, s 9.
[22]Rudraksh Lakra, Medha Kolanu and Abhijeet Shrivastava, 'Data, Control, and Power: Decoding India's Digital Personal Data Protection Act, 2023' (SSRN Working Paper, 2025).

Protection Board.

An economic analysis prepared by CUTS International specifically assessed the financial costs of the verifiable-parental-consent mechanisms contemplated by the Act and the then-draft Rules, and found that government-ID-based verification could cost a platform in the region of INR 1.5 crore per million verifications annually, while DigiLocker-based verification could cost approximately INR 30 lakh per million verifications annually.[23] Even the lower figure represents a substantial absolute compliance expenditure for a platform with tens or hundreds of millions of users - a scale not unusual among Indian social media, ed-tech, gaming, or e-commerce platforms - and one that may ultimately be passed on to consumers, limiting access to affordable digital services. The report further highlights the risk that this burden falls disproportionately on resource-constrained start-ups relative to incumbent platforms able to spread the same fixed infrastructure costs over a larger revenue base. Industry representations made well before the Rules were finalised anticipated this concern, noting that several jurisdictions had struggled for nearly a decade to scale age-verification systems to hundreds of millions of users, and that industry would need to build new application programming interfaces, prototype age-verification systems, and test their accuracy and security before launch.

This paper's concern is that the absence of graded obligations, regulatory sandboxes, and financial support mechanisms risks limiting innovation and raising entry barriers - a concern squarely implicated by Section 9 and the Rules made under it. The DPDP Act does, elsewhere, recognise the principle of graded obligations: Section 10[24] establishes the category of "Significant Data Fiduciary," to be notified by the Central Government based on the volume and sensitivity of personal data processed, the risk to Data Principals' rights, and considerations of sovereignty and security, imposing more stringent obligations - including the appointment of a Data Protection Officer and an independent data auditor, and the conduct of data protection impact assessments - on such entities. By contrast, the verifiable-parental-consent requirement under Section 9[25] applies identically to a five-person ed-tech start-up and to a billion-user social media company, save that the Rules' allowance for reliance on an existing verified parental

[23] Aayush Iqubbal and Kavya Jugiani, 'Economic Analysis of Verifiable Parental Consent Mechanisms: Evaluating Impact on Consumers and Data Fiduciaries' (CUTS International, 2025).
[24] Digital Personal Data Protection Act 2023, s 10.
[25] Digital Personal Data Protection Act 2023, s 9.

account is, by definition, unavailable to a new entrant with no existing user base.

Neither the Act nor the Rules provide anything resembling a regulatory sandbox - a mechanism, familiar from the financial sector, that allows smaller or lower-risk entities to test compliance approaches in a supervised, relaxed environment before full implementation is required. The staggered commencement addresses only the timing of obligations, not their distribution: all Data Fiduciaries, irrespective of size, bear the same substantive obligation from the same date, subject only to a general - and, under Section 9(5),[26] largely theoretical - exemption where the Central Government is satisfied that processing is being carried out "in a verifiably safe manner." The existence of a verification ecosystem is thus presumed rather than subsidised, and the decision to grant or withhold exemption proceeds on that presumption. The absence of any subsidised or shared verification infrastructure - such as a low-cost, centralised age-verification utility forming part of a broader innovation ecosystem for start-ups - leaves the financial-support dimension of this concern unaddressed as of the date the Rules were published.

V. State Exemptions under Section 17: Necessity, Proportionality, and the Puttaswamy Standard

Several commentators have identified Section 17 of the DPDP Act[27] as the provision most in tension with the constitutional reasoning in Puttaswamy. Most of the Act's substantive obligations are relaxed where processing is required for the enforcement of legal rights or claims (Section 17(1)), or by courts and tribunals in the exercise of judicial functions (Section 17(2)). Section 17(2) is considerably broader: it permits the Central Government to exempt the processing of personal data by any instrumentality of the State from all or any provisions of the Act, on grounds of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, the maintenance of public order, or the prevention of incitement to the commission of any cognisable offence relating to any of these.

Two difficulties arise from this text. First, the grounds enumerated - "sovereignty," "integrity," "security of the State," "public order" - mirror those in Article 19(2) of the Constitution,[28] which governs reasonable restrictions on freedom of speech, yet have not

[26]Digital Personal Data Protection Act 2023, s 9(5).
[27]Digital Personal Data Protection Act 2023, s 17.
[28]Constitution of India, art 19(2).

acquired any settled meaning in that context despite decades of jurisprudence. No statutory definition of these terms exists for the purposes of Section 17, leaving the executive considerable latitude in determining whether the threshold for exemption has been met.

Second, and more significant for the proportionality analysis, an exemption under Section 17(2)[29] does not depend on the specific obligation that a given State interest justifies setting aside; rather, once notified, it operates to exempt the relevant instrumentality from "all or any" provisions of the Act. This stands in contrast to the treatment of lawful interception as an exception to data-protection obligations under the Information Technology Act, 2000, which provides only for specific, time-limited interception of particular communications under defined procedures. A notification under Section 17(2)[30] is thus considerably less proportionate and specific than Puttaswamy contemplates, amounting to a wholesale exclusion of an entity from the data-protection framework, without any continuing duty - save, in some formulations, to keep security measures "reasonable" - and without any mechanism for periodic review, sunset, or judicial oversight of the notification itself.

Private actors, too, may be exempted from compliance with Sections 17(3)[31] and 17(5)[32] in certain circumstances. Section 17 is thus not confined to State instrumentalities: the Central Government may exempt Data Fiduciaries, including start-ups, from specified obligations - such as the duty to give notice under Section 5 before seeking consent - for a defined class of Data Fiduciaries and to the extent prescribed. Section 17(5) is broader still, allowing the Central Government to exempt any Data Fiduciary or class of Data Fiduciaries from any provision of the Act, for any period, during the five years following the Act's commencement (that is, until August 2028). This power remained unused as of early 2026, but had already attracted lobbying from large digital-payments companies seeking relief that would ease constraints on their use of publicly available information to train artificial-intelligence models and to process digital transactions.

These provisions sit in instructive juxtaposition. Section 17(2) permits the State to exempt itself from the Act on grounds of sovereignty and security - a step that Puttaswamy would require to meet the strictest justificatory standard, given that the State is the actor most capable

[29]Digital Personal Data Protection Act 2023, s 17(2).
[30]Digital Personal Data Protection Act 2023, s 17(2).
[31]Digital Personal Data Protection Act 2023, s 17(3).
[32]Digital Personal Data Protection Act 2023, s 17(5).

of intruding upon informational privacy at scale and systematically. At the same time, Sections 17(3) and 17(5) confer a broad power on the Central Government to exempt private actors - including dominant commercial platforms - from obligations designed to protect individuals from those very actors. As one commentator has observed, the result is that restrictions on a constitutionally recognised fundamental right are not confined to narrow, judicially defined exceptions, but instead constitute reservoirs of executive discretion available to the State and to favoured private parties alike.[33]

VI. "Certain Legitimate Uses" under Section 7: Consent by Default?

Section 4 of the DPDP Act permits the processing of personal data only for a lawful purpose, and only where one of two conditions is satisfied: either the Data Principal consents to the processing (Section 6), or the processing falls within one of the "certain legitimate uses" enumerated in Section 7. Section 7 sets out nine categories - including the voluntary provision of personal data for a specified purpose, processing necessary for the performance of functions of the State, processing pursuant to legal orders, processing for medical emergencies, and processing for employment-related purposes - within which a Data Fiduciary may process personal data without consent. This closed-list approach differs from Article 6(1)(f) of the GDPR, which permits processing on the basis of a "legitimate interest" determined through a fact-specific balancing test between the interests of the data subject and those of the processing party - a mechanism absent from the DPDP Act.[34]

The first, and in practice most significant, of the nine categories is Section 7(a), which permits processing where the Data Principal has "voluntarily provided" personal data to a Data Fiduciary for a specified purpose, without indicating that she does not consent to its use for that purpose. Read literally, this provision could extend to a wide range of ordinary transactions: a customer providing a phone number to a pharmacy for a payment receipt, a patient providing particulars at a hospital reception desk, or a borrower providing know-your-customer information on a loan application - in each case, information is voluntarily provided without express refusal.[35] The difficulty is that almost any data furnished in the course of a transaction may be characterised as "voluntary" in this sense, since overt coercion is rarely present; if Section 7(a) were construed broadly, it would become the basis for processing relied

[33] Abhishek Singh and Anushka (n 19).
[34] Graham Greenleaf (n 17).
[35] Abhishek Singh and Anushka (n 19).

upon in nearly all consumer transactions, relegating the more elaborate consent framework of Section 6 to a residual category of cases in which a Data Fiduciary chooses, for whatever reason, not to invoke Section 7(a).

The interaction between Section 7(a) and Section 6(6)[36] compounds this tension, since a Data Fiduciary may continue to process personal data collected before the Act's commencement until the Data Principal withdraws consent, even where that data was originally collected in a manner inconsistent with the standards the Act now prescribes for consent. On one reading, Sections 6(6) and 7(a) together establish a latent route to implied consent: the absence of any indication of non-consent is treated as equivalent to consent, in apparent tension with the "clear affirmative action" standard required by Section 6.[37] This concern is not confined to any single sector - finance, healthcare, e-commerce, or telecommunications - but, as one commentator has observed, represents a latent compliance risk capable of affecting the entire regulated economy, since Data Fiduciaries, in good faith or otherwise, may process data in ways a Data Principal never contemplated when "voluntarily" providing it for an entirely unrelated and more limited purpose.

As of this writing, the Data Protection Board of India has offered no express clarification on this issue, nor does the Act itself provide guidance. This paper submits that Section 7(a) ought to be construed narrowly, consistent with the general principle of Indian administrative and constitutional law that exceptions to a statutory right should be read as narrowly as possible, with the right treated as the norm and the exception as a genuine exception - such that processing under Section 7(a) is confined to the purpose expressly communicated to the Data Principal at the time the data was voluntarily provided. On this reading, the pharmacy in the illustration above may use a customer's phone number to send a payment receipt, but may not use that number for marketing communications absent a separate ground under Section 7 or separate consent. Whether this narrow construction prevails, or whether Section 7(a) instead becomes, through administrative practice, a general-purpose consent bypass, is likely to be among the most consequential interpretive questions to arise once the Act's substantive provisions take effect in May 2027.

[36]Digital Personal Data Protection Act 2023, s 6(6).
[37]R.K. Singh and Vini Singh, 'Beyond Consent: Ensuring Meaningful Protection of Genetic Data Under India's Digital Personal Data Protection Act, 2023' (2025) Statute Law Review (advance online publication).

VII. The Absent "Sensitive Personal Data" Category: Health and Financial Data

One of the more significant structural choices in the DPDP Act is its departure from the earlier framework under the Information Technology Act, 2000, in not carrying forward a standalone category of "sensitive personal data" - a category that had singled out financial information, health conditions, biometric data, sexual orientation, and similar categories for heightened protection, and that had also appeared in the 2021 Joint Parliamentary Committee's draft Rules.[38] Instead, the Act adopts a risk-based approach, imposing heightened obligations on entities designated "Significant Data Fiduciaries" by the Central Government, based, among other factors, on the volume and sensitivity of the personal data processed (Section 10).[39]

In the healthcare context, the practical effect is that the same statutory provisions apply irrespective of the sensitivity of the data being processed - in the same manner as they would to an e-commerce platform processing names and delivery addresses - unless and until the Central Government prescribes otherwise, or the entity in question is separately notified as a Significant Data Fiduciary, a determination that, as of the Rules' notification, remains largely unspecified for most sectors.[40] This marks a significant departure from the 2021 Joint Parliamentary Committee draft, which would have imposed heightened obligations - including explicit consent and data-localisation requirements - on entities collecting health data, as a form of "sensitive personal data." This shift raises the question whether the absence of a distinct sensitive-data category will permit State instrumentalities and private corporations to apply a lower standard of care to medical records than their sensitivity warrants, particularly given the continued operation of parallel health-data governance frameworks such as the Ayushman Bharat Digital Mission, whose relationship with the DPDP Act's erasure, consent, and retention provisions remains unreconciled.

The financial sector presents a similarly complex picture, given the extensive body of sectoral regulation administered by the Reserve Bank of India, the Securities and Exchange Board of India, and the Insurance Regulatory and Development Authority of India, which, combined with the absence of a sensitive-personal-data category, produces an uneven regulatory landscape. The most evident conflict concerns data retention and erasure. The DPDP

[38]Vasudha Khanna and Atul Kotwal, 'Examining the Significance of the Digital Personal Data Protection Act, 2023 in the Context of the Healthcare Industry: A Comprehensive Analysis' (2025) (working paper).
[39]Digital Personal Data Protection Act 2023, s 10.
[40]Douwe Korff, 'The Indian Digital Personal Data Protection Act, 2023, Viewed from a European Perspective' (SSRN, 2023).

Act confers on Data Principals the right to seek erasure of personal data no longer necessary for the purpose for which it was processed, yet Reserve Bank of India regulations require banks, non-banking financial companies, and other regulated entities to retain know-your-customer records and transaction data for prescribed periods that cannot be overridden by an erasure request under the DPDP Act.[41] The DPDP Rules, 2025 partially address this tension by prescribing default retention periods for several categories of entities in the Third Schedule - for instance, three years from the last transaction or login for e-commerce and social-media entities with at least two crore registered Indian users, and for online-gaming entities with at least fifty lakh registered users - but the Schedule does not purport to reconcile all sectoral retention obligations with the DPDP erasure right, leaving regulated entities to determine, on a case-by-case basis, which of two or more retention regimes applies to a given category of data.

The scenarios the Data Protection Board has indicated it may consider in assessing penalties are illustrative of this friction: a digital bank retaining know-your-customer information beyond the period permitted under the DPDP framework - even where such retention purports to comply with Reserve Bank of India directions - may nonetheless face a significant penalty from the Board if the retention is found to exceed the scope permitted under the DPDP regime, leaving open the prospect that a regulated entity may receive contradictory directions from two regulators concerning the same data.[42]

VIII. Implementation Architecture: The DPDP Rules, 2025 and the Compliance Roadmap

Much of the foregoing analysis concerns provisions of the DPDP Rules, 2025, and it is accordingly useful to consider the broader architecture of their implementation. The substantive obligations and rights discussed in Parts III to VI above - including the consent provisions, child-data-protection obligations, and exemption provisions - were brought into force on a staggered basis, taking effect eighteen months after notification (14 May 2027), while other, largely institutional provisions came into force immediately upon notification on 14 November 2025. Provisions concerning Consent Managers occupy an intermediate position, with an effective date twelve months after notification (14 November 2026).

The consequence of this staggered commencement is that the Data Protection Board will

[41] Douwe Korff (n 40).
[42] ibid.

exist and operate for a considerable period (from November 2025 to May 2027) before the substantive obligations it is tasked with monitoring take effect. The Rules supply considerable operational detail to the bare text of the Act: Rule 6 prescribes "reasonable security safeguards"; Rule 7 sets out the process for breach notification, including a seventy-two-hour reporting window that has attracted particular commentary; Rule 8 and the Third Schedule govern retention and erasure - the Third Schedule sets a three-year retention ceiling, measured from the Data Principal's last interaction, for e-commerce and social-media entities with at least two crore registered Indian users and for online-gaming entities with at least fifty lakh registered users, discussed in Part VII above; Rules 10 and 11 operationalise verifiable parental consent as discussed in Part IV; and Rule 15, together with the notification requirement in Section 16 of the Act, introduces a "negative list" approach to cross-border data transfers - a list that, as of early 2026, remains unpublished, leaving the default position (that cross-border transfers are permitted) in full force pending publication of its principal exception.

The scale of the applicable penalties underscores the significance of this implementation phase. The Schedule to the Act caps penalties at ₹250 crore for failure to implement reasonable security safeguards under Section 8(5), and at ₹200 crore for breach of the special obligations owed to children under Section 9 - among the highest fixed-sum penalties in any data-protection statute worldwide. The eighteen-month period until May 2027 represents a window of opportunity for the Data Protection Board, the Central Government (through further rule-making or clarificatory guidance), and the courts (in the pending Supreme Court litigation and any follow-on proceedings) to resolve the structural ambiguities identified in this paper before an incorrect interpretation becomes entrenched under the threat of penalties of this magnitude.

IX. Towards Reform: Interpretive and Legislative Recommendations

The analysis above suggests two categories of deficiency, calling for two corresponding categories of response. Some deficiencies do not arise from ambiguity in the statutory text and can, in principle, be resolved through guidance from the Data Protection Board of India or through judicial interpretation, without legislative amendment. Others stem from deliberate drafting choices - such as the exclusion of juristic persons from "Data Principal" status, the absence of a sensitive-personal-data category, and the absence of a right to data portability or a right to be forgotten - and can be resolved only through amendment.

First, with respect to Section 7(a), the Data Protection Board should, at minimum, adopt

and articulate a narrow interpretation - whether in formal guidance, in response to the pending Supreme Court litigation, or through adjudicatory orders - confirming that "voluntary provision" for a "specified purpose" is confined to that purpose, and that the absence of an express indication of non-consent should not be read as authorising processing for any other purpose, including one merely "closely related." Such guidance would not require legislative enactment, yet would substantially reduce the likelihood that Section 7(a) becomes, in practice, a general consent-bypass provision.

Second, in relation to the treatment of corporate and proprietorship personal data discussed in Part III, the Central Government could, under its general rule-making power, provide specific guidance on business-to-business processing - for instance, by clarifying that the personal data of a sole proprietor processed in the course of business may be treated as that person's personal data for DPDP purposes, while separately guiding counterparty enterprises on their legitimate interests in controlling downstream use of personal data received in a commercial relationship, including through template contracts or codes of conduct for commerce and industry.[43]

Third, the disproportionate burden borne by start-ups and small businesses in implementing verifiable parental consent, discussed in Part IV, calls for a tiered-obligations system analogous to the existing Significant Data Fiduciary framework. This could be achieved through delegated provisions permitting smaller platforms to rely on lighter verification measures - such as self-declaration coupled with audit - for a defined period, before transitioning to more rigorous government-ID or DigiLocker-based verification. The government might concurrently develop DigiLocker-based verification infrastructure, contemplated by the Rules as one of two principal verification routes, and make it available to qualifying start-ups on subsidised or free terms. Such measures would directly address the cost concerns identified in the CUTS International analysis without compromising the substantive child-protection guarantees of Section 9.[44]

Fourth, the breadth of the Section 17 exemption power is the defect most clearly warranting constitutional reform - not because of any particular instance of its use, but because its constitutional vulnerability lies in the generality of the power itself, to disapply the Act

[43]Douwe Korff (n 40).
[44]Aayush Iqubbal and Kavya Jugiani (n 23).

wholesale. A reform consistent with the Puttaswamy proportionality standard would confine Section 17(2) exemptions to specific provisions of the Act, rather than the Act in its entirety, and would subject such exemptions to a review mechanism - whether parliamentary, through a committee analogous to those scrutinising delegated legislation, or judicial - beyond the general remedy of a writ petition. Pending such legislative reform, the Central Government could, within its existing rule-making powers, adopt this calibrated approach in structuring future Section 17(2) notifications, thereby strengthening its position in the pending constitutional litigation.

Fifth, the absence of a sensitive-personal-data category, and the consequent friction with sectoral regulators discussed in Part VII, could be addressed through a more modest remedy: a rule-making power - which the Act's general delegation provisions appear sufficiently wide to accommodate - enabling the Central Government to direct that the processing of specified categories of data (health, financial, or biometric data) in compliance with corresponding sectoral obligations be deemed compliant with the corresponding DPDP obligation, thereby establishing a harmonisation mechanism. Finally, the absence of data portability and of a standalone right to be forgotten is a consequence of the Act's architecture at its highest level, and would require amendment of the Act itself; in the interim, the Data Protection Board could, within the existing erasure framework under Section 12, encourage Significant Data Fiduciaries, as a matter of good practice rather than legal obligation, to provide data in portable formats upon request - thereby achieving some of the competitive benefits of a portability right through soft-law means, pending future legislative reconsideration.

X. Conclusion

The Digital Personal Data Protection Act, 2023, together with the Digital Personal Data Protection Rules, 2025, is unquestionably a significant step: India's first comprehensive, cross-sectoral data protection legislation, enacted in the wake of, and in explicit response to, the Supreme Court's recognition of informational privacy as an incident of the fundamental right to life and personal liberty in Puttaswamy. Yet, as this paper has sought to demonstrate, the distance between the Act's constitutional promise and its statutory text is greater than the preamble suggests. The narrow definition of “Data Principal” means that personal data flowing through India's vast commercial and institutional structures - that of company directors, proprietors, employees, and vendor representatives - is regulated by a framework that does not

account for that structure. While the verifiable-parental-consent mandate is well-intentioned and designed to protect children, it has been implemented through Rules that impose disproportionate compliance costs relative to child-protective benefit on entities of widely varying size, without any tapering of obligations or shared infrastructure to reconcile child protection with the Act's stated aim of enabling a digital economy. The Section 17 State-exemption power and the unresolved consent-bypass potential of Section 7(a) together suggest that the Act's consent architecture - its principal GDPR-inspired feature - is, in practice, more open to circumvention than its guiding principles suggest. Viewed against the earlier drafts of 2018 and 2021, the DPDP Act, 2023 emerges as the product of numerous decisions to simplify, narrow, and, in certain respects, exclude particular rights of Data Principals - decisions whose cumulative impact on those rights has not, this paper argues, been fully appreciated.

This is not to suggest that the DPDP Act is a "failed or illegitimate exercise of the legislative power" within the meaning of Puttaswamy, nor that the Act ought to have replicated the complexity of the 2018 and 2021 drafts, a level of detail that may well have proved counterproductive on its own terms. The argument advanced here is more targeted: the specific deficiencies identified - concerning State and private exemptions, the scope of legitimate uses, the treatment of juristic persons, and the absence of sector-specific safeguards - are real, textually grounded, and material, and the eighteen months between the Act's commencement and the substantive provisions taking effect in May 2027 represent a limited but genuine opportunity for the Data Protection Board of India, the Central Government, and ultimately the Supreme Court to close the gap between the Act's text and the technology, commerce, and constitutional values it is intended to govern.