© MAY 2026 | IRE Journals | Volume 9 Issue 11 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I11-1718085

Consent, Control, and the Constitution: Deconstructing India's Digital Personal Data Protection Act, 2023

ROHAN S
BBA LL.B. (Hons.), Amity Law School, Noida

Abstract*—The enactment of the Digital Personal Data Protection Act (DPDPA), 2023, marks the culmination of India's long and contested legislative journey toward a statutory data protection regime. Built upon the constitutional bedrock of the right to privacy affirmed in K.S. Puttaswamy (Retd.) v. Union of India (2017), the Act nominally centres the individual as the sovereign of her personal data. Yet a close doctrinal reading reveals a regime in which consent — the Act's primary lawful basis for processing — is structurally compromised by broadly drawn "deemed consent" provisions, an absence of genuine withdrawal mechanisms, and a regulatory architecture that subordinates individual control to state and commercial interests. This paper interrogates the DPDPA's consent framework as a site of constitutional tension, examining whether the Act's design meets the proportionality standard mandated by Puttaswamy and provides meaningful individual control over personal data in an age of algorithmic surveillance. Through doctrinal analysis and comparative reference to the GDPR and the California Consumer Privacy Act, this paper argues that the DPDPA's consent framework is constitutionally underspecified and recommends six targeted legislative remedies to restore the individual to the centre of India's data governance design.

Keywords- DPDPA 2023, Consent, Data Fiduciary, Puttaswamy, Fundamental Rights, GDPR, Informational Privacy

I. INTRODUCTION

On 11 August 2023, India's Parliament enacted the Digital Personal Data Protection Act — a statute that its architects described as a citizen-centric instrument designed to balance "the right of individuals to protect their personal data" with "the need to process personal data for lawful purposes." This stated ambition places consent at the normative heart of the legislation: if individuals are to be the sovereigns of their data, then their agreement to its collection and use must be genuine, informed, freely given, and revocable. The reality, as this paper demonstrates, is considerably more complicated.

Consent has long occupied a paradoxical position in data protection law globally. It is simultaneously the most rights-respecting basis for data processing — because it preserves individual autonomy — and the most easily manipulated — because power asymmetries between individuals and large data processors render "free" consent fictitious. The GDPR's architects grappled with this paradox by building structural constraints around consent: granularity requirements, the prohibition on bundled consent, ease of withdrawal, and alternative lawful bases reducing dependence on consent for routine processing. India's DPDPA imports the rhetoric of consent but not its structural disciplines.

This paper proceeds in five substantive parts. Part II situates the DPDPA's consent framework within the constitutional jurisprudence of privacy, focusing on *Puttaswamy*'s proportionality mandate. Part III undertakes a granular doctrinal analysis of the Act's consent and deemed consent provisions, identifying structural infirmities. Part IV examines the regulatory architecture.

Part V offers comparative perspectives. Part VI concludes with recommendations.

"A consent regime structurally incapable of being freely given or meaningfully withdrawn is not a privacy protection — it is a legitimation device."

II. THE CONSTITUTIONAL ARCHITECTURE OF CONSENT: PUTTASWAMY AND PROPORTIONALITY

The nine-judge bench in *Puttaswamy* (2017) 10 SCC 1 settled that privacy is a fundamental right under Article 21, overruling the earlier decisions in *M.P. Sharma v. Satish Chandra* AIR 1954 SC 300 and *Kharak Singh v. State of U.P.* AIR 1963 SC 1295. Crucially, Justice D.Y. Chandrachud's lead opinion identified *informational self-determination* — the right of individuals to control information about themselves — as a constitutionally protected dimension of privacy. This doctrine forms the constitutional foundation upon which any data protection statute must be evaluated.

A. The Proportionality Standard

Any legislative action curtailing informational privacy must satisfy the four-limb proportionality test: (i) *legality* — a law authorising the interference; (ii) *legitimate aim* — a valid state objective; (iii) *necessity* — the minimum restriction necessary; and (iv) *proportionality stricto sensu* — benefit must outweigh harm to the right. Drawn from European constitutional methodology and the German *Verhältnismäßigkeit* doctrine, this test, subsequently applied in *Anuradha Bhasin v. Union of India* (2020) 3 SCC 637 and the Aadhaar judgment, sets the constitutional standard against which the DPDPA's consent derogations must be assessed.

B. Informational Self-Determination as Positive Obligation

Justice Chandrachud further held that the State bears not merely a negative duty to abstain from privacy violations but a positive obligation to create legal conditions for individuals to exercise informational self-determination. This positive dimension is constitutionally significant: a data protection statute must affirmatively empower individuals to exercise control, not merely confer paper rights that cannot be practically enforced. An Act that provides a right to withdraw consent under Section 6(4) but fails to specify operational timelines or mechanisms arguably fails this constitutional obligation.

C. The Consent Fiction: Lessons from Puttaswamy (Aadhaar)

Justice Chandrachud's dissent in the Aadhaar judgment observed that consent extracted under conditions of practical compulsion — such as conditioning welfare benefits upon biometric enrolment — is constitutionally indistinguishable from coercion. This analysis is directly applicable to the DPDPA's context, where digital access to essential services, employment, and civic participation may become conditioned on "consent" to data processing, rendering consent a mere formality rather than a genuine exercise of autonomy.

III. ANATOMY OF THE DPDPA'S CONSENT FRAMEWORK: DOCTRINAL ANALYSIS

A. The Consent Standard Under Section 6

Section 6(1) of the DPDPA requires that consent be "free, specific, informed, unconditional and unambiguous," expressed through a "clear affirmative action." This is broadly aligned with GDPR Article 7. However, the Act's consent regime lacks several structural disciplines that give the GDPR's consent standard its practical rigour. First, the DPDPA does not explicitly prohibit "bundled consent" — conditioning an entire service on a single omnibus consent covering multiple distinct processing purposes. GDPR Recital 43 expressly provides that consent should not be valid where processing is "bundled with the performance of a contract." India's omission creates a significant loophole for platforms to deploy all-or-nothing consent gates incompatible with the "specific" and "free" requirements.

B. Withdrawal of Consent: The Operationalisation Gap

Section 6(4) provides that a data principal "may withdraw her consent at any time." However, the DPDPA is silent on the timeframe within which a data fiduciary must give effect to withdrawal, the technical mechanisms that must be available, and consequences of non-compliance beyond the general grievance mechanism. The GDPR's Article 17 right to erasure, triggered upon withdrawal of consent, is absent in the DPDPA — or at best implied in the qualified right to erasure under Section 13. This operationalisation gap renders the right to withdraw consent structurally weak in practice.

C. The Deemed Consent Provisions: A Consent Surplus?

Section 7 of the DPDPA creates seven categories of "deemed consent" under which personal data may be processed without explicit consent. These include performance of state functions, compliance with legal obligations, medical emergencies, employment purposes, and — most significantly — "any other legitimate use as may be prescribed." The last category effectively delegates the scope of the Act's primary safeguard to the Central Government through subordinate legislation, creating a consent bypass of uncertain and potentially vast ambit. The GDPR's "legitimate interests" ground under Article 6(1)(f) — the closest comparator — is subject to a three-part balancing test, cannot be relied upon by public authorities in the exercise of their tasks, and has been extensively constrained by CJEU jurisprudence. India's "legitimate use" carve-out lacks all of these structural constraints.

© MAY 2026 | IRE Journals | Volume 9 Issue 11 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I11-1718085

IV. REGULATORY ARCHITECTURE AND THE ENFORCEMENT DEFICIT

A. The Data Protection Board: Institutional Design Critique

Section 18 of the DPDPA establishes the Data Protection Board of India (DPB) as the adjudicatory authority. Members are appointed by the Central Government, which also determines their salaries, terms of service, and grounds of removal. This design departs significantly from GDPR Article 52(1)'s mandate that each supervisory authority must "act with complete independence" — a requirement the CJEU has interpreted strictly, invalidating national provisions conferring executive influence over appointment or tenure (*Commission v. Germany*, C-518/07). Executive control over the Board's constitution directly compromises consent enforcement: if the largest data fiduciary in India is the State itself — through Aadhaar, GSTN, and the Ayushman Bharat digital health stack — the Board's capacity to enforce consent requirements against government data processors depends entirely on its operational independence.

B. Penalty Architecture: Deterrence or Optics?

Schedule I of the DPDPA specifies penalties of up to ■250 crore (approximately €27 million) for breach of security safeguard obligations. While significant in absolute terms, the deterrent effect is limited for large global platforms. The GDPR's ceiling of €20 million or 4% of global annual turnover translates to €1.2 billion for a company with €30 billion in global revenue — as demonstrated by the Irish DPC's 2023 €1.2 billion penalty against Meta. India's fixed-ceiling approach systematically under-deters large data fiduciaries while potentially over-deterring small domestic operators, inverting the regulatory risk calculus.

Consent Parameter	DPDPA 2023	GDPR (EU)	Assessment
Consent Standard	Free, specific, informed, unconditional, unambiguous (S.6(1))	Freely given, specific, informed, unambiguous (Art.7)	*Broadly equivalent; GDPR adds operational guidance via Recitals*
Bundled Consent	Not prohibited; gap in Rules	Expressly prohibited (Recital 43; Art.7(4))	*DPDPA deficient; loophole for platforms*
Withdrawal Right	Any time (S.6(4)); no timeline prescribed	Any time, as easy as giving (Art.7(3))	*DPDPA lacks operational discipline*
Deemed Consent / Legitimate Interests	7 grounds + open-ended "legitimate use" (S.7)	6(1)(f): 3-part balancing; not for public authorities	*DPDPA significantly broader; no balancing required*
Supervisory Authority	DPB: executive-appointed; quasi-judicial body	Independent DPA; complete independence (Art.52)	*DPDPA structurally deficient; independence not guaranteed*
Penalty Regime	Up to ■250 cr (fixed) ≈ €27M (Schedule I)	Up to €20M or 4% global turnover (Art.83)	*DPDPA under-deters large global platforms*

Table 1: Comparative Consent Framework — DPDPA 2023 vs. GDPR

V. THE SURVEILLANCE DIMENSION: SECTION 17 AND THE NULLIFICATION OF CONSENT

Section 17 of the DPDPA empowers the Central Government to exempt any instrumentality of the State from the Act's obligations in the interests of sovereignty, security of the State, friendly relations with foreign states, maintenance of public order, or prevention of incitement to cognisable offences. This exemption is categorical and unqualified: it is not subject to proportionality review by the Board, does not require a reasoned order, and contains no sunset clause or periodic review requirement.

The constitutional problem with Section 17 is structural: the same government that is the largest data fiduciary in India has unilateral power to exempt itself from the consent requirements that bind private actors. In *Puttaswamy*, Justice Chandrachud observed that "the right of privacy is a right against the State as much as it is against non-State actors." Section 17 inverts this constitutional logic, creating an asymmetric regime in which private data fiduciaries are bound by consent disciplines that the State can unilaterally discard. This asymmetry cannot be justified under the necessity limb of the proportionality test: if national security requires derogation from consent requirements, that derogation must be specific, targeted, and judicially reviewable — not a blanket executive power of indefinite scope.

Comparative constitutional law offers instructive contrasts. The GDPR's national security exemption under Article 23 permits restrictions only by legislative measure that "respects the essence of the fundamental rights and freedoms" and constitutes a "necessary and proportionate measure in a democratic society." The CJEU's decision in *Schrems II* (C-311/18, 2020) demonstrated the Court will scrutinise even parliamentary-enacted derogations with rigour. India's Section 17, operating through executive notification with no equivalent parliamentary or judicial check, represents a regime more consistent with executive supremacism than constitutional privacy protection.

"Section 17 does not balance privacy against national security — it subordinates the former to the latter by executive fiat, without the proportionality discipline that the Constitution demands."

VI. TOWARD A CONSTITUTIONALLY COHERENT CONSENT FRAMEWORK: RECOMMENDATIONS

The foregoing analysis identifies six specific legislative reforms necessary to bring the DPDPA's consent framework into alignment with the *Puttaswamy* constitutional mandate and global best practice:

1. Amendment to Section 6: Prohibition on Bundled Consent
Section 6 should expressly prohibit conditioning service provision on consent to processing not necessary for performance of the service, mirroring GDPR Article 7(4). Rules should specify that consent for distinct processing purposes must be sought separately, with granular opt-in mechanisms for each identified purpose.

2. Amendment to Section 6(4): Operationalising Withdrawal
Section 6(4) should require data fiduciaries to give effect to consent withdrawal within prescribed periods (suggested: 72 hours for cessation of processing; 30 days for erasure). Fiduciaries must provide a dedicated, technically reliable withdrawal mechanism — not merely a general grievance email.

3. Amendment to Section 7: Constraining Deemed Consent
The "legitimate use" category under Section 7 should be subject to a statutory balancing test: the processing must be necessary for a legitimate purpose, must not override fundamental rights of the data principal, and must be accompanied by the ability to object. Government instrumentalities should be expressly prohibited from relying on "legitimate use" as a processing ground.

4. Reconstitution of the Data Protection Board
Section 18 should establish the Board as a fully independent statutory authority, with members appointed by a collegium comprising the Chief Justice of India (or nominee), the Comptroller and Auditor General, and the Chairperson of the National Human Rights Commission — with security of tenure and parliamentary funding.

5. Amendment to Section 17: Proportionate Surveillance Derogation
Any exemption of State instrumentalities must: (i) be authorised by specific parliamentary statute; (ii) be subject to independent judicial review within 30 days; (iii) be time-limited with mandatory parliamentary renewal; and (iv) be limited to specific processing activities satisfying the necessity and proportionality limbs of the Puttaswamy test.

6. Introduction of Portability and Algorithmic Rights
The DPDPA should introduce: (i) a right to data portability in structured, machine-readable format; and (ii) a right to object to processing for direct marketing and a right to human review of consequential automated decisions — laying the groundwork for AI accountability before a future

Digital India Act addresses the broader algorithmic governance landscape.

VII. CONCLUSION

The Digital Personal Data Protection Act, 2023, arrives at a pivotal moment in India's democratic life. The right to privacy has been constitutionally affirmed. The digital economy has placed personal data at the centre of economic value creation. The State's surveillance capabilities have expanded dramatically. In this context, a data protection statute that genuinely operationalises consent as a mechanism of individual control would be a landmark achievement of constitutional governance. The DPDPA is not that statute — yet.

The Act's consent architecture, while nominally aligned with global standards, is undermined by the breadth of its deemed consent provisions, the absence of structural disciplines against bundled or coerced consent, the operationalisation gap in withdrawal rights, and — most fundamentally — the Section 17 exemption that removes the State from the Act's ambit entirely. The Board's institutional design, which subordinates its independence to executive control, further compromises the enforceability of whatever consent protections the Act does provide.

The path forward is not the wholesale rejection of the Act but its constitutionally disciplined reform. The six recommendations advanced in Part VI are targeted, doctrinal, and achievable through amendment, grounded not in abstract aspiration but in the constitutional obligations that *Puttaswamy* has already imposed. India's data governance framework will be judged not by the sophistication of its statutory language but by whether its citizens experience genuine control over their personal data. That experience begins, and must begin, with consent.

REFERENCES

A. Cases and Judgments

[1] K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., (2017) 10 SCC 1 [Nine-Judge Privacy Bench].
[2] K.S. Puttaswamy v. Union of India, (2019) 1 SCC 1 [Aadhaar Five-Judge Bench].
[3] Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.
[4] M.P. Sharma v. Satish Chandra, District Magistrate, Delhi, AIR 1954 SC 300.
[5] Kharak Singh v. State of U.P., AIR 1963 SC 1295.
[6] Shreya Singhal v. Union of India, (2015) 5 SCC 1.
[7] Case C-518/07, Commission v. Germany [2010] ECR I-1885 (CJEU) [DPA Independence].
[8] Case C-311/18, Data Protection Commissioner v. Facebook Ireland (Schrems II), ECLI:EU:C:2020:559 (CJEU 2020).
[9] Case C-673/17, Planet49 GmbH v. Bundesverband der Verbraucherzentralen, ECLI:EU:C:2019:801 (CJEU 2019).

B. Legislation and Instruments

[10] Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023) (India).
[11] Information Technology Act, 2000 (Act No. 21 of 2000) (India).
[12] Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (India).
[13] Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1.
[14] California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100–1798.199.100 (2018, as amended by CPRA 2020).
[15] UK Data Protection Act 2018 (c.12); Age Appropriate Design Code (Children's Code), ICO (UK, 2020).

C. Official Reports

[16] Justice B.N. Srikrishna Committee, 'A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians' (MeitY, Government of India, July 2018).
[17] Joint Parliamentary Committee on the Personal Data Protection Bill, 2019, Report (Lok Sabha Secretariat, December 2021).
[18] European Data Protection Board, 'Guidelines 05/2020 on Consent under Regulation 2016/679' (EDPB, Version 1.1, 4 May 2020).
[19] Article 29 Working Party, 'Guidelines on Consent under Regulation 2016/679' (WP259 rev.01, April 2018).

D. Books and Journal Articles

[20] Graham Greenleaf, *Asian Data Privacy Laws: Trade and Human Rights Perspectives* (OUP, 2014).
[21] Rahul Matthan, *Privacy 3.0: Unlocking Our Data-Driven Future* (HarperCollins India, 2018).
[22] Eleni Kosta, *Consent in European Data Protection Law* (Martinus Nijhoff Publishers, 2013).
[23] Vrinda Bhandari and Renuka Sane, 'Towards a Privacy Framework for India in the Age of the Internet' (2018) 14 Journal of Indian Law and Society 1.
[24] Arnav Kumar, 'The Chimera of Consent: Consent-Based Data Protection Under India's DPDPA, 2023' (2024) 9 Indian Journal of Law and Technology 45.
[25] Paul Schwartz and Daniel Solove, 'The PII Problem' (2011) 86 New York University Law Review 1814.
[26] Usha Ramanathan, 'A Unique Identity Bill: Concerns' (2010) 45(35) Economic and Political Weekly 10.
[27] Apar Gupta, 'Surveillance Law and Technology in India: An Analysis of the DPDPA's Section 17 Exemption' (2024) 11 NUJS Law Review 88.
[28] Rohan Suraj, 'The Deemed Consent Problem: Structural Deficits in India's Data Protection Act' (2025) 9(1) Amity International Journal of Juridical Sciences 45.