

INTERNATIONAL JOURNAL OF LAW
MANAGEMENT & HUMANITIES
[ISSN 2581-5369]

Volume 9 | Issue 4

2026

© 2026 International Journal of Law Management & Humanities

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of any suggestions or complaints, kindly contact support@vidhiaagaz.com.

To submit your Manuscript for Publication in the International Journal of Law Management & Humanities, kindly email your Manuscript to submission@ijlmh.com.

Granularity of Consent under the Digital Personal Data Protection Act, 2023

PRATYUSH PANDEY*

ABSTRACT

This paper offers a doctrinal, comparative, and constitutional analysis of Section 6 of the Digital Personal Data Protection Act, 2023, which requires consent to be free, specific, informed, unconditional and unambiguous. It asks whether a single, bundled “accept all” consent mechanism satisfies these requirements. Drawing on textual statutory interpretation, comparative EU materials (the GDPR and European Data Protection Board guidance), and India’s constitutional privacy jurisprudence, the paper argues that bundled consent is doctrinally inconsistent with Section 6. It proposes a bright-line interpretive standard that treats “specific” as purpose-segmented consent, and sets operational criteria (necessity, conditionality, granularity, affirmative action, and ease of withdrawal) for regulators and courts. The paper concludes with practical compliance and enforcement recommendations for platforms and the Data Protection Board.

Keywords: DPDP Act, consent, bundled consent, granular consent, Section 6, GDPR, EDPB, Planet49, Puttaswamy, informational autonomy

I. INTRODUCTION

Consent sits at the centre of the statutory architecture created by the Digital Personal Data Protection Act, 2023 (hereafter “the Act”).¹ Section 6 prescribes that the consent of the Data Principal must be “free, specific, informed, unconditional and unambiguous, with a clear affirmative action”.² In everyday digital practice, however, the dominant model remains the bundled “accept all” flow: a single click that authorises multiple, often functionally and temporally distinct, processing activities. This research asks a narrow doctrinal question with broad consequences: does Section 6 permit omnibus, bundled consent, or must consent be granular, that is, segmented by purpose and processing operation? The answer shapes platform

* Author is an Advocate at High Court of Chhattisgarh, Bilaspur, Chhattisgarh, India.

¹ The Digital Personal Data Protection Act, 2023, No. 22 of 2023, Acts of Parliament, 2023 (India). The Act has been brought into force in stages: Section 2 and Sections 18 to 26 (among others) with effect from 13 November 2025; sub-section (9) of Section 6, on the registration of Consent Managers, with effect from 13 November 2026; and Sections 3 to 5, sub-sections (1) to (8) and (10) of Section 6, and Sections 7 to 17, with effect from 13 May 2027. See MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY, Notification G.S.R. 843(E) (13 November 2025).

² *Id.* § 6(1).

design, regulatory enforcement, and the meaningfulness of informational autonomy for Indian Data Principals.

This paper proceeds in four parts. The first offers a close textual reading of Section 6 and the related statutory scaffolding. The second situates the Indian statutory text against European jurisprudence and guidance (the GDPR and the European Data Protection Board) and the Court of Justice of the European Union's *Planet49* ruling on pre-checked consent. The third situates the debate within India's constitutional privacy doctrine, especially the informational autonomy principles articulated in *K.S. Puttaswamy*.³ The fourth proposes an interpretive standard and practical tests for courts and regulators, and concludes with compliance implications.

II. TEXTUAL AND DOCTRINAL READING OF SECTION 6

A. The Statutory Language and Immediate Implications

Section 6(1) of the Act requires consent that is “free, specific, informed, unconditional and unambiguous with a clear affirmative action”, and limits consent to processing that is “for the specified purpose and be limited to such personal data as is necessary for such specified purpose”.⁴ Two textual elements are salient:

- “Specific”: the adjective is located adjacent to “informed” and “unconditional”, indicating the legislature’s intention to demand a precision of purpose and scope; and
- “Limited to such personal data as is necessary for such specified purpose”: a built-in proportionality and necessity requirement that links consent to the data minimisation principle.

A literalist reading therefore provides immediate doctrinal support for the view that consent must be more than a ritualistic click: it must be tethered to specific purposes and constrained by necessity.

B. Statutory Silence and Interpretive Constraints

The Act does not define “specific”, or explain whether the word mandates purpose-wise toggles or simply a reasonably intelligible statement of multiple purposes.⁵ This silence leaves courts and the Data Protection Board with interpretive work: whether to read Section 6 as requiring granularity (separate consents for distinct processing activities) or as allowing bundled-but-

³ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).

⁴ Digital Personal Data Protection Act, 2023, *supra* note 1, § 6(1).

⁵ See Digital Personal Data Protection Act, 2023, *supra* note 1, § 2. The Act defines “specified purpose” in Section 2(z) as “the purpose mentioned in the notice given by the Data Fiduciary to the Data Principal in accordance with the provisions of this Act and the rules made thereunder”, but it does not define “specific”.

notified consent, where multiple purposes are described in one notice but obtained by a single affirmative action.

Two interpretive constraints are germane. First, statutory terms that engage fundamental rights ought to be read generously in favour of protecting autonomy, consistent with constitutional readings of privacy. Secondly, the Act's internal cross-references to necessity and limitation suggest that "specific" cannot be hollow, in the sense that it cannot merely be ornamental language attached to an "accept all" button.

III. COMPARATIVE LAW: GDPR, EDPB AND PLANET49

A. The GDPR Framework and EDPB Guidance

The GDPR requires consent to be "freely given, specific, informed and unambiguous".⁶ Article 7 and recital 32 emphasise active and informed action, and Article 7(4) specifically warns against conditionality, where consent to processing that is not necessary for the contract is made a precondition for the service.⁷ The European Data Protection Board's guidelines on consent elaborate that "bundling" consent with other terms, and "tying" service provision to unnecessary data processing, can vitiate the voluntary nature of consent; the EDPB treats granularity as best practice and often as legally required in contexts where multiple, distinct processing operations are proposed.⁸

The EDPB's more recent opinions (for example, on "consent-or-pay" constructs) have reinforced that consent cannot be a mere transactional escape hatch that absolves controllers of other GDPR duties. When consent is the chosen legal basis, controllers must show real choice, the ability to refuse, and the ability to accept or refuse specific purposes granularly.⁹ These doctrinal concerns are mirrored in empirical work showing that users rarely exercise granular choices even when they are presented, tending instead to accept bundled consent dialogues.¹⁰

⁶ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1, art. 4(11).

⁷ *Id.* art. 7(4) and recital 32. Recital 32 provides that consent is presumed not to be freely given where it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or where the performance of a contract, including the provision of a service, is made dependent on consent that is not necessary for that performance.

⁸ EUROPEAN DATA PROTECTION BOARD, *Guidelines 05/2020 on Consent under Regulation 2016/679*, version 1.1 (adopted 4 May 2020).

⁹ EUROPEAN DATA PROTECTION BOARD, *Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms* (adopted 17 April 2024).

¹⁰ Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub & Thorsten Holz, *(Un)informed Consent: Studying GDPR Consent Notices in the Field*, in PROCEEDINGS OF THE 2019 ACM SIGSAC CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY 973 (2019).

B. Planet49 and Active Consent

The Court of Justice of the European Union's decision in *Planet49* confirmed that pre-ticked boxes do not amount to valid consent, emphasising active, affirmative behaviour by the data subject.¹¹ While *Planet49* is framed around cookies, its doctrinal logic on active consent and on the opacity of aggregated consent choices has broader applicability to bundled consent regimes.¹²

C. Lessons for India's Act

Although the Digital Personal Data Protection Act, 2023 does not explicitly reproduce the GDPR's jurisprudence, the close textual consonance on consent elements, and the common law's reliance on reasoned comparative materials, mean that the EDPB's granular approach and *Planet49*'s emphasis on affirmative action are strong interpretive tools. Where the Act is ambiguous, comparative materials can be instructive to courts and the Data Protection Board when construing "specific" and "unconditional".

IV. CONSTITUTIONAL DIMENSION: INFORMATIONAL AUTONOMY AND PROPORTIONALITY

A. Informational Privacy as Autonomy

The Supreme Court in *K.S. Puttaswamy*¹³ recognised the right to privacy as part of the fundamental right under Article 21. The judgment grounds informational privacy in dignity and autonomy, and applies the proportionality test for state intrusions. While the Act governs private flows predominantly, the constitutional principle of informational autonomy provides normative weight: where statutory regimes affect the ability of individuals to control personal data, courts should construe statutory language in a manner that preserves meaningful choice.

Seen through this lens, consent is not merely a contractual device or a compliance box to tick, but a mechanism through which the individual's status as an autonomous rights-bearer is recognised in the data economy. In *Puttaswamy*, the Court rejected both statist and market-centric accounts that treat personal data as a tradable commodity, stressing instead that informational self-determination is intrinsic to personhood. If privacy is about the right to be left alone, and also about the ability to decide how, when, and to what extent information about oneself is shared, then a regime that permits coarse, all-or-nothing consent sits uneasily with

¹¹ Case C-673/17, *Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband eV v. Planet49 GmbH*, ECLI:EU:C:2019:801 (CJEU, Grand Chamber, 1 October 2019).

¹² Klaus Wiedemann, *The ECJ's Decision in "Planet49" (Case C-673/17): A Cookie Monster or Much Ado About Nothing?*, 51 INTERNATIONAL REVIEW OF INTELLECTUAL PROPERTY AND COMPETITION LAW 543 (2020).

¹³ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, *supra* note 3.

this constitutional commitment. Bundled “accept all” flows, which compel individuals to consent to multiple, heterogeneous purposes at once, reduce their role to that of passive data sources rather than active choosers.

This has direct implications for how Section 6 should be read. The Act’s requirement that consent be “free, specific, informed, unconditional and unambiguous” can be understood as a statutory attempt to operationalise the autonomy-centred vision of privacy articulated in *Puttaswamy*. “Free” reflects the concern that consent obtained under coercion, structural dependence, or take-it-or-leave-it conditions is not genuinely voluntary. “Specific” and “informed” aim to ensure that individuals are not forced to gamble with broad, indeterminate permissions, but can calibrate their exposure to different kinds of processing. “Unconditional” underscores that access to essential or core services cannot be made contingent on acquiescing to unrelated surveillance.¹⁴ Read together, these elements transform consent from a thin, formal authorisation into a thicker practice of respecting user agency.

Granularity is the practical expression of this transformation. A person can only exercise meaningful informational autonomy if she can say “yes” to some uses and “no” to others without having to withdraw from the digital sphere altogether. In a world where participation in platforms, payments, and communications is often unavoidable, the choice between “share everything” and “opt out of the service entirely” is illusory. Granular consent, meaning separate and intelligible choices for materially different purposes, allows individuals to align data flows with their own values, sensitivities, and risk appetites. A user may, for example, be comfortable with data processing necessary to deliver a messaging service, but unwilling to permit cross-context behavioural profiling for targeted advertising. A constitutional understanding of autonomy insists that the law create space for such differentiated choices rather than forcing them into a single bundled click.

Puttaswamy’s proportionality framework also supports this reading at a structural level. Although the case concerns state action, its logic is that any limitation on privacy should pursue a legitimate aim, be suitable and necessary, and impair rights in the least restrictive way. When Parliament enacts a data protection statute that shapes the baseline for private data flows, courts can legitimately import these values as interpretive guides. If controllers can achieve their aims by offering separate toggles for distinct purposes, there is little justification for insisting on a bundled “accept all” mechanism that maximises data extraction at the cost of individual control. In other words, where two interpretations of Section 6 are available, one that tolerates omnibus

¹⁴ EUROPEAN DATA PROTECTION BOARD, *supra* note 8 (on conditionality, and on the bundling of consent with the provision of a service).

consent and one that requires purpose-segmented consent, the proportionality-infused understanding of informational autonomy counsels in favour of the latter.

Grounding Section 6 in informational autonomy helps to answer the charge that granular consent is an imported or excessively “European” standard. The claim advanced here is not that Indian law must mirror the GDPR because Europe demands it, but that the core features of granular consent resonate with India’s own constitutional trajectory: a trajectory that places dignity, autonomy, and the capacity to shape one’s digital footprint at the heart of privacy. On this view, the question is not whether Indian courts should borrow foreign doctrine, but whether they are willing to let the statutory language of “free” and “specific” be read so narrowly that it undermines the very autonomy that *Puttaswamy* sought to secure.

B. Proportionality and Consent Architecture

Two aspects of proportionality are relevant to the consent architecture:

- Suitability and necessity: consent should be linked to what is necessary for the stated purpose, and bundling extraneous processing with necessary processing risks failing the necessity limb;¹⁵ and
- Least restrictive means: if there are less intrusive means to achieve the controller’s goals (for example, obtaining separate consent toggles for distinct purposes), then bundling cannot be justified merely by administrative convenience.

Applying these constitutional values to Section 6 recommends reading “specific” as a requirement that protects the Data Principal’s informational autonomy against coarse, aggregated choices.

V. TOWARDS AN INTERPRETIVE STANDARD FOR GRANULAR CONSENT

To move from critique to prescription, this Part proposes a doctrinal standard, the “Granularity and Conditionality Test”, that courts and the Data Protection Board can use to decide whether a bundled consent mechanism passes muster.

A. The Granularity and Conditionality Test (GCT): Elements

- Purpose segmentation (granularity): consent must be mapped to clearly separable purposes. Where controllers propose materially distinct processing operations (for example, core service delivery, targeted advertising, or research resale), each such purpose requires its own affirmative consent toggle. A combined notice that lists many

¹⁵ Digital Personal Data Protection Act, 2023, *supra* note 1, § 6(1) (consent must be “limited to such personal data as is necessary for such specified purpose”); EUROPEAN DATA PROTECTION BOARD, *supra* note 8.

purposes but provides only one “accept all” action fails this element. Meskenaitė similarly reads “specific” consent as requiring a clear link between each purpose and a separate act of consent, rather than broad, bundled permissions.¹⁶

- Necessity and proportionality: for each proposed purpose, the controller must show that the personal data requested is necessary for that purpose. Where processing is not necessary for service performance, it must not be tied coercively to service provision (see conditionality).
- Conditionality test (refusal consequences): controllers may only condition service provision on consent where the processing is strictly necessary for the service. If refusal of optional processing results in disproportionate denial of service (functional lock-in), consent is not “free”. The Data Principal must be able to refuse the optional purpose without losing access to the core service.
- Affirmative action and unambiguity: the mechanism must require an active and demonstrable affirmative action for each optional purpose, with no pre-ticked boxes and no silence as consent. The mechanism must be traceable and auditable by the controller.¹⁷
- Accessibility of withdrawal and granular withdrawal: withdrawal must be as easy as giving consent. Importantly, withdrawal should apply at the granularity at which consent was obtained, so that a toggle for targeted advertising is withdrawable without affecting other consents.¹⁸
- Clarity of notice (informed): notices must be intelligible and short-form for the key elements, namely purpose, data types, consequences of refusal, retention, and remedies. Dense legalese, or “notice dumping” into an opaque policy, undermines “informed”.¹⁹

¹⁶ Gabbi Meskenaitė, *An Examination of the Criteria for Valid Consent under the GDPR in the Light of the Rationale and Technological Neutrality* (Master’s thesis, Department of Law, Faculty of Law, Lund University, 2022), Lund University Publications.

¹⁷ Digital Personal Data Protection Act, 2023, *supra* note 1, § 6(1) (consent must be unambiguous and given “with a clear affirmative action”); *Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband eV v. Planet49 GmbH*, *supra* note 11.

¹⁸ Digital Personal Data Protection Act, 2023, *supra* note 1, §§ 6(4) to 6(6) (the Data Principal may withdraw consent at any time, and on withdrawal the Data Fiduciary must, within a reasonable time, cease and cause its Data Processors to cease processing) and § 6(7) (consent may be given, managed, reviewed or withdrawn through a Consent Manager); GDPR, *supra* note 6, art. 7(3) (it must be as easy to withdraw as to give consent).

¹⁹ Digital Personal Data Protection Act, 2023, *supra* note 1, §§ 5 and 6(3) (notice of the personal data and the purpose of processing, and requests for consent in clear and plain language, with the option of English or any language specified in the Eighth Schedule); Digital Personal Data Protection Rules, 2025, G.S.R. 846(E) (13 November 2025), r. 3 (the notice must be presented, and be understandable, independently of any other information made available by the Data Fiduciary). Rule 3 comes into force on 13 May 2027, and Rule 4, on the registration and obligations of Consent Managers, on 13 November 2026.

B. Illustrative Application of the GCT

- Example 1, a health app: core processing (appointment scheduling) as against targeted health-insurance offers. Under the GCT, separate toggles are required, and refusal of marketing toggles cannot disable appointment functionality.
- Example 2, a messaging platform: processing for account provision as against profiling for advertisement personalisation. The latter requires granular consent, and account provision cannot be made conditional on consenting to profiling.

C. Burden of Proof and Accountability

When consent is the legal basis, the controller should bear the burden of demonstrating compliance with Section 6, including that consents were obtained separately where required. This comports with the “demonstrable” standard in Article 7(1) of the GDPR and with the Act’s own accountability ethos.²⁰

VI. ENFORCEMENT, COMPLIANCE AND PRACTICAL IMPLICATIONS

A. For the Data Protection Board and Adjudication

The Data Protection Board should adopt the GCT as a normative enforcement framework. Remedies could range from requiring controllers to redesign consent flows to monetary penalties for the systematic bundling of optional processing.²¹ Interpreting Section 6 through the GCT aligns statutory text, comparative guidance, and constitutional values.

B. For Platforms and Designers

- Interface design: platforms should implement toggles for materially distinct processing activities, and ensure that toggles are independent and not buried.
- Default settings: defaults should favour privacy. Opt-out defaults should be used only where legally justified, but because the Act pushes for affirmative action, opt-in is the safer route.
- Consent logging: controllers should log granular consents with timestamps and purpose identifiers to meet accountability and evidentiary needs.
- Business models: advertising-funded models may need reconfiguration, since “consent or pay” models will be scrutinised under conditionality principles and EDPB guidance.

²⁰ GDPR, *supra* note 6, art. 7(1); Digital Personal Data Protection Act, 2023, *supra* note 1, § 6(10) (where consent is the basis of processing and a question arises in a proceeding, the Data Fiduciary is obliged to prove that notice was given and that consent was obtained in accordance with the Act) and § 8(1).

²¹ Digital Personal Data Protection Act, 2023, *supra* note 1, § 33 read with the Schedule.

C. Limits and Edge Cases

- Technical bundling for efficiency: minor operational bundling that does not materially expand the data used or the purposes pursued (for example, a single screen that lists tight, related sub-purposes) may survive the GCT if user choice remains meaningful.
- Inferred data and cross-purpose use: where controllers wish to repurpose data (for example, from transaction analytics to behavioural profiling), fresh consent is required unless a different lawful basis, other than consent, is demonstrably applicable.²² In the mental health context, for instance, commentators have stressed layered, granular consent and easy withdrawal as key safeguards against coercive or confusing consent flows.²³

VII. OBJECTIONS AND RESPONSES

A. Objection 1: Administrative Burden and Consent Fatigue

Response: the administrative cost is real, but the alternative is hollow consent that undermines legal legitimacy. Better interface design, through layered notices and progressive disclosure, reduces user fatigue while preserving granularity.

B. Objection 2: Commercial Viability (Pay-or-Consent)

Response: EDPB guidance and emerging jurisprudence show scepticism towards coercive “consent-or-pay” schemes, and the Act’s “free” requirement counsels against extortionate models.²⁴ Regulators can permit differentiated pricing only when refusal genuinely does not affect access to essential functionality.

C. Objection 3: Global Interoperability

Response: convergence with GDPR practices reduces friction, and Indian controllers serving global markets already adapt to granular consent models. The GDPR offers a useful comparative benchmark against which the Act can be assessed, and Indian consent standards should therefore be interpreted in a manner that is interoperable with, and not materially weaker than, the established EU requirements of specificity, granularity, and genuine choice.²⁵

²² Digital Personal Data Protection Act, 2023, *supra* note 1, §§ 4 and 7 (personal data may be processed only for a lawful purpose for which the Data Principal has given consent, or for a certain legitimate use).

²³ Manik Inder Singh Sethi, Narayana Manjunatha, Naveen Kumar Channaveerachari, Tanmoy Chakraborty, Suresh Bada Math & Chittaranjan Andrade, *The Digital Personal Data Protection Act 2023: Implications for Mental Healthcare Practice in India*, INDIAN JOURNAL OF PSYCHOLOGICAL MEDICINE (online first, 10 September 2025), doi: 10.1177/02537176251370651.

²⁴ EUROPEAN DATA PROTECTION BOARD, *supra* note 9.

²⁵ GDPR, *supra* note 6, arts. 4(11) and 7(4), and recital 32; EUROPEAN DATA PROTECTION BOARD, *supra* note 8.

VIII. CONCLUSION

The analysis in this paper suggests that Section 6 of the Digital Personal Data Protection Act, 2023 cannot be reconciled with omnibus “accept all” flows for materially distinct processing activities. Read textually, the requirement that consent be “specific” and limited to what is “necessary for such specified purpose” points away from coarse, aggregated authorisations and towards purpose-linked, constrained permissions. When this statutory language is placed alongside the structure of the Act and its emphasis on necessity and limitation, bundled consent emerges less as a drafting gap and more as a practice that sits uneasily with the Act’s own internal logic.

Comparative materials reinforce this reading rather than dilute it. GDPR doctrine, EDPB guidance on bundling and conditionality, and the *Planet49* judgment collectively treat granularity, real choice, and active, purpose-wise consent as core to the very idea of valid consent, not as optional design flourishes. The Granularity and Conditionality Test proposed in this paper translates those insights into an Indian statutory context without mechanically importing foreign law. It offers regulators and courts a structured way to distinguish between legitimate operational bundling and unlawful attempts to smuggle multiple, optional processing operations behind a single affirmative act.

India’s constitutional privacy jurisprudence adds a further, and independent, reason for caution about bundled consent. If informational privacy is an aspect of dignity and autonomy, and if proportionality is the standard for justifying intrusions, then statutory ambiguities that affect control over personal data should be resolved in favour of preserving meaningful choice. On that view, granular consent is not simply a compliance preference but a constitutional orientation: it is the mechanism through which individuals retain agency over which aspects of their lives are rendered legible to digital intermediaries.

At the same time, the paper has acknowledged that granular consent carries costs. Controllers must redesign interfaces, rethink defaults, and accept that some lucrative secondary uses will require genuine, and therefore sometimes withheld, permission. These burdens are real, and they risk being dismissed as “formalism” or “European overreach” if they are presented without sensitivity to local business models and infrastructural constraints. The more constructive path, sketched here, is to treat granularity as a design constraint that can coexist with innovation, through layered notices, purpose-wise toggles for high-impact processing, and careful calibration of when consent is the appropriate legal basis at all.

Ultimately, the paper's claim is modest but firm. Section 6, properly interpreted, does not outlaw every instance of bundled interaction with users, nor does it mandate an explosion of checkboxes for trivial operational distinctions. It does, however, require that where controllers propose materially different purposes, especially those involving profiling, cross-context tracking, or sensitive data, they secure consent at the level at which people meaningfully experience risk. For courts, the Data Protection Board, and designers, the question going forward is less whether granularity is desirable in the abstract, and more how far they are willing to let convenience erode the Act's promise that consent will be both legally valid and experientially real.
