STATE EXEMPTIONS UNDER THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023: TESTING SECTION 17(2)(A) AGAINST THE PROPORTIONALITY STANDARD

Yash Verma, Advocate, Delhi High Court

ABSTRACT

The Digital Personal Data Protection Act, 2023 builds its architecture around consent, yet Section 17 carves out exemptions that sit uneasily with that architecture. Among these, Section 17(2)(a) stands apart. It allows the Central Government to exempt any instrumentality of the State from the whole of the Act, not merely from specific chapters, on grounds such as sovereignty, security, and public order, through nothing more than an executive notification. This paper examines whether that power survives the proportionality standard laid down in Justice K.S. Puttaswamy v Union of India and refined in later decisions such as Anuradha Bhasin v Union of India. It argues that Section 17(2)(a) fails at the standard's third and fourth limbs, it dispenses with any calibrated, least-intrusive design, and it builds in no procedural safeguard against misuse, unlike the framework the Supreme Court itself read into telephone tapping law in PUCL v Union of India. The paper situates this gap within the institutional design of the Data Protection Board of India, whose Chairperson and Members are selected entirely through executive-controlled committees, and argues that this makes correction more urgent, not less. Drawing a comparison with Article 23 of the GDPR and India's own precedent in PUCL, the paper closes with concrete proposals, a defined class of instrumentality, a sunset clause, and a recorded-reasons requirement, all of which the Rules notified in November 2025 currently omit.

Keywords: Digital Personal Data Protection Act; Section 17; State exemptions; proportionality standard; right to privacy; Data Protection Board of India.

Introduction

India's first comprehensive data protection statute rests on a fairly simple premise: personal data cannot be processed without either the consent of the person it belongs to, or a specific statutory ground that dispenses with consent.[1] The Digital Personal Data Protection Act, 2023 spends its opening sections building this architecture with some care, defining personal data, defining who counts as a Data Fiduciary, and setting out what a valid notice and a valid consent must look like. Then Section 17 arrives and quietly hollows out a large part of it.

Section 17 contains five distinct exemption powers, ranging from narrow and defensible, processing needed to enforce a legal claim, or to investigate a defaulting borrower's assets, to sweeping and largely unexamined.[2] This paper is concerned with Section 17(2)(a), which lets the Central Government notify any "instrumentality of the State" as exempt from the entire Act, not merely from the notice and consent requirements in Chapters II and III, on grounds of sovereignty, integrity, security of the State, friendly relations with foreign States, public order, or preventing incitement to offences connected with these.[3] Nothing in the Act defines "instrumentality of the State" for this purpose, nothing requires the notification to carry a time limit, and nothing in the Digital Personal Data Protection Rules, 2025, notified on 13 November 2025, attaches any procedural condition to how the power is exercised.[4]

This matters because the Act was drafted, at least on paper, to give legislative form to the right to privacy that a nine-judge bench recognised in Justice K.S. Puttaswamy v Union of India.[5] That judgment did not simply declare privacy a fundamental right and stop there. It set out a method for testing State action that restricts privacy, a method the Court has applied and sharpened since.[6] This paper asks a narrow question: does Section 17(2)(a) survive that method? It argues that it does not, and that the reasons are fixable, through judicial reading-in of safeguards along lines the Court has already used for telephone interception, or through specific amendments to the Rules before the provision becomes practically significant. That window is closing faster than the Act's own commencement structure suggests, for reasons this

[1] The Digital Personal Data Protection Act, 2023, No. 22 of 2023, §§ 4, 6 (India)..
[2] Id. § 17
[3] Id. § 17(2)(a).
[4] Ministry of Electronics and Information Technology, Digital Personal Data Protection Rules, 2025 (Nov. 13, 2025) (India).
[5] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
[6] K.S. Puttaswamy v. Union of India, (2019) 1 SCC 1 (India); Anuradha Bhasin v. Union of India, (2020) 3 SCC 637 (India).

paper returns to at the end.

Mapping the Exemption

Section 17 is best read as five separate mechanisms rather than one. Section 17(1) lists six situations, enforcing a legal right, judicial or regulatory functions, law enforcement investigation, cross-border outsourcing contracts, court-approved corporate restructuring, and assessing a loan defaulter's assets, in which Chapter II obligations (barring the Data Fiduciary's core accountability and security duties under Section 8(1) and 8(5)), Chapter III, and Section 16's cross-border transfer rules do not apply.[7] These are targeted carve-outs tied to specific activity, each with a reasonable analogue elsewhere.

Section 17(3) lets the government notify certain classes of Data Fiduciary, startups among them, as exempt from specific provisions, a targeted power that, as of this writing, has not yet been exercised.[8] Section 17(5) is broader: it lets the government exempt any Data Fiduciary or class from any provision for a specified period, but Parliament capped its own power here, it lapses five years after commencement, so it must be used, if at all, by August 2028.[9]

Section 17(2) changes the structure entirely. Unlike 17(1), 17(3), and 17(5), it does not list which provisions are disapplied, it disapplies the whole Act. Clause (a) covers processing by a notified instrumentality of the State, and, notably, processing by the Central Government itself of any data that instrumentality chooses to pass on to it.[10] Clause (b) is narrower, a partial exemption for research, archiving, and statistical processing, conditioned on the data not being used for a decision about a specific individual and on safeguards the government is meant to prescribe, safeguards that, as of this writing, remain unprescribed.[11] Section 17(4) adds a further, standing carve-out for the State: even without a 17(2)(a) notification, State processing is exempt from the erasure duty in Section 8(7) and, unless the processing affects a decision about the individual, from the right to information under Section 12(2) and the right to erasure under Section 12(3).[12]

---

7 The Digital Personal Data Protection Act, 2023, § 17(1)(a)-(f).
8 Id. § 17(3); see also DPDP Act Exemptions: When the Law Does Not Apply, ComplyZero (Feb. 6, 2026), https://www.complyzero.com/blog/dpdp-act-exemptions-explained.
9 Id. § 17(5).
10 Id. § 17(2)(a).
11 Id. § 17(2)(b).
12 Id. § 17(4).

Taken together, a notified instrumentality under Section 17(2)(a) faces no consent requirement, no purpose limitation, no data minimisation duty, no accuracy obligation, no retention limit, and no principal-facing right of access, correction, or erasure. What survives is the duty to secure the data reasonably and to remain accountable for a processor's conduct, since Sections 8(1) and 8(5) continue to bind regardless of any Section 17 exemption.[13] Everything else sits at the government's discretion, switched on by a single notification the Act does not require to be time-bound, reasoned in public, or placed before Parliament.

The Standard Puttaswamy Set

The nine-judge bench in Puttaswamy did not leave the content of the right to privacy to be worked out case by case with no guiding method. Several of the opinions converged on a structured test for State action restricting privacy, later distilled into four related enquiries.[14] First, is there a law, meaning a validly enacted statute, that authorises the restriction. Second, does that law pursue a legitimate State aim, something beyond mere administrative convenience. Third, is the restriction proportionate to that aim, in the sense of being the least intrusive way of achieving it, with a rational connection between means and end. Fourth, does the framework include safeguards against arbitrary use, so the restriction is not left to unstructured executive discretion.

The Court applied a version of this method to the Aadhaar framework in 2019, upholding some provisions and striking down others depending on whether each cleared the third and fourth limbs.[15] It applied a similar structure in Anuradha Bhasin v Union of India when reviewing internet shutdown orders in Jammu and Kashmir, holding that a restriction on a fundamental right needs a rational nexus to its stated purpose, must be the least restrictive option reasonably available, and must carry some mechanism for review.[16] The common thread is that the first two limbs, a valid law and a legitimate aim, are usually easy for the State to satisfy. The real scrutiny happens at the third and fourth: is the restriction narrowly tailored, and can it be checked.

It is worth being precise about what the test does not require. It does not require that the State be barred from processing personal data for security or public order purposes, and nobody

[13] Id. § 17(1) proviso (retaining §§ 8(1), 8(5)).
[14] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
[15] K.S. Puttaswamy v. Union of India, (2019) 1 SCC 1 (India).
[16] Anuradha Bhasin v. Union of India, (2020) 3 SCC 637 (India).

seriously argues that intelligence or law enforcement agencies should operate under the same consent architecture as an e-commerce platform. The test asks something narrower: given that some departure from the ordinary rules is justified, is this particular departure calibrated to what is actually necessary, and is there a way to catch its misuse. That is the standard against which Section 17(2)(a) has to be measured, and it is on this narrower question that the provision runs into real difficulty.

Testing Section 17(2)(a)

On the first limb, legality, Section 17(2)(a) clears the bar in form. It is a power created by a validly enacted statute, and the Act requires it to be exercised through a notification, which at least ensures the exemption is publicly recorded once made.

The second limb, legitimate aim, is also met on the face of the provision. Sovereignty, integrity, security of the State, and public order are the same grounds Article 19(2) of the Constitution already treats as legitimate bases for restricting other fundamental rights.[17] The trouble is how broadly these grounds have historically been read. Commentary on the Bill's earlier drafts pointed out that terms like sovereignty and integrity are undefined anywhere in the Act, and that "instrumentality of the State" could extend, on the Supreme Court's own tests for what counts as State under Article 12, to any body under the government's deep and pervasive control, a category wide enough to include public undertakings with no plausible security function.[18] A legitimate aim stated at this level of generality does little work in practice, since almost any processing can be redescribed as serving public order or security if the redescription is never tested against anything.

It is the third limb, proportionality in the narrow sense, where Section 17(2)(a) is hardest to defend. A calibrated version of this power would exempt a notified instrumentality from specific obligations that genuinely conflict with a security or law enforcement function, the way Section 17(1) does for investigation and prosecution. Instead, Section 17(2)(a) exempts the instrumentality from the Act altogether. There is no requirement that the exemption track the specific processing activity that justifies it, none that it expire or be reviewed, and none of

---

[17] India Const. art. 19(2).

[18] India's Data Protection Law Allows Government to Exempt Itself, MediaNama (Aug. 3, 2023), https://www.medianama.com/2023/08/223-dpdp-bill-2023-government-exemptions-3/; Ajay Hasia v. Khalid Mujib Sehravardi, (1981) 1 SCC 722 (India).

the sunset that Section 17(5) imposes on exemptions granted to private Data Fiduciaries.[19] A private company seeking relief from the Act is capped at a defined period and a defined set of provisions. A government instrumentality seeking the same relief faces no such limit once notified. A framework more generous to the State than to a startup sits awkwardly with a standard that asks whether the chosen restriction is the least intrusive one available.

The fourth limb, procedural safeguards, is where the gap is clearest. Nothing in the Act or the 2025 Rules requires the government to record its reasons for a Section 17(2)(a) notification in a form open to challenge, to review the notification periodically, to report on how the exemption has been used, or to route the decision through a body independent of the notifying ministry. Compare the framework the Supreme Court itself built for telephone interception in PUCL v Union of India, where, faced with a similarly open-ended power under Section 5(2) of the Indian Telegraph Act, 1885, the Court read in procedural conditions: interception orders had to be reviewed by a committee headed by the Cabinet Secretary, had to state reasons, and their necessity had to be reassessed every two months.[20] The Court did this because a power capable of being used for surveillance cannot safely depend on executive self-restraint alone. Section 17(2)(a) creates a power at least as capable of that use, over a far larger volume of data than telephone intercepts ever generated, and currently carries none of the safeguards PUCL required for a narrower power thirty years earlier.

An Adjudicator Answering to the Same Executive

A natural response to this gap is that the Data Protection Board of India exists precisely to check this kind of overreach, and that a complaint about a State instrumentality's data practices can, in principle, reach the Board. The difficulty is that the Board's own design does not yet support that role.

Section 19 of the Act provides that the Board's Chairperson and Members are appointed by the Central Government, and the 2025 Rules fill in how.[21] Two Search-cum-Selection Committees recommend names, one for the Chairperson, chaired by the Cabinet Secretary and including the Secretaries of the Ministry of Electronics and Information Technology and the Department of Legal Affairs, and one for the other Members, chaired by the MeitY Secretary along with

[19] The Digital Personal Data Protection Act, 2023, § 17(5).
[20] People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301 (India).
[21] The Digital Personal Data Protection Act, 2023, § 19.

the Legal Affairs Secretary, each rounded out by two government-selected experts.[22] Every seat on both committees is either a serving civil servant or an expert the government itself chooses. Nothing requires a nominee of the Chief Justice of India or any other judicial voice in the process, even though the Board exercises powers equivalent to a civil court and its orders are appealable only to a specialised tribunal.[23] The Competition Act, 2002, by contrast, requires the selection committee for the Competition Commission to be chaired by the Chief Justice of India or a nominee, precisely because Parliament recognised that a body with adjudicatory power needs a selection process insulated from the executive it may have to rule against.[24] The DPDP Act had that model available and chose not to use it.

This is not a hypothetical concern. Government-appointed selection committees were still working through the process of recommending the Board's Chairperson and Members well into 2026.[25] A Board built this way, asked to adjudicate a complaint against the very government that appointed it and that controls the ministry proposing to notify it as exempt, is not the independent check that would ordinarily be expected to compensate for weak safeguards elsewhere in the statute. If anything, this raises the stakes for getting the safeguards right at the point Section 17(2)(a) is exercised, since the usual downstream check is compromised from the outset.

What Other Systems Require

India is not the first jurisdiction to face the tension between State access to personal data and a rights-based protection framework. Article 23 of the General Data Protection Regulation permits EU member states to restrict data subject rights for reasons including national security, defence, and public security, but only through a legislative measure that is itself necessary and proportionate, and only if that measure specifies the categories of data and processing affected, the scope of the restriction, safeguards against abuse, and the storage periods and review arrangements that apply.[26] The comparison is imperfect, the GDPR sits within a different constitutional structure, but the underlying design choice, that a restriction serving State interests should itself be bounded and reviewable rather than open-ended, is a general one, not

[22] Digital Personal Data Protection Rules, 2025, r. 17.
[23] The Digital Personal Data Protection Act, 2023, §§ 28(7), 29.
[24] The Competition Act, 2002, No. 12 of 2003, § 9(1)(a) (India).
[25] MeitY Plans to Cut Short DPDP Compliance Timeline and Notify Cross Border Restrictions for SDFs, S.S. Rana & Co. (Feb. 17, 2026), https://ssrana.in/articles/meity-plans-to-cut-short-dpdp-compliance-timeline-and-notifycross-border-restrictions-for-sdfs/.
[26] Regulation (EU) 2016/679, General Data Protection Regulation, art. 23.

a peculiarity of European law.

India has, in fact, already built exactly this kind of structure once, in a different context. PUCL did not strike down Section 5(2) of the Telegraph Act. It kept the power intact and built a procedural cage around it, because the Court recognised that surveillance powers left unchecked, however legitimate their stated purpose, tend to expand in practice.[27] There is no reason that lesson stops short of Section 17(2)(a). The government does not need to lose the power to exempt its instrumentalities from ordinary data protection rules where genuinely necessary. It needs to exercise that power inside a structure that makes misuse visible and correctable, which is a different thing from the power being unlimited.

What Would Fix It

Three changes would bring Section 17(2)(a) much closer to what Puttaswamy and its progeny require, and none need Parliament to reopen the Act, since each could plausibly be implemented through the Rules or through a notification format the government adopts on its own.

First, a notification under Section 17(2)(a) should be tied to a defined, published class of instrumentalities and specific processing activities, rather than a general grant covering an entire agency's operations. This would track the Section 17(1) model, which is activity-specific, and would stop the definitional uncertainty around "instrumentality of the State" from becoming a route to open-ended exemption.

Second, every notification should carry a fixed term, renewable only on a fresh notification with recorded reasons, mirroring the five-year cap Parliament itself imposed on Section 17(5) for private Data Fiduciaries. There is no principled reason the State should operate under a looser standard than the one it set for everyone else.

Third, the Rules should require that a notification under Section 17(2)(a) be accompanied by a statement of reasons, placed before Parliament the way subordinate legislation ordinarily is, and reviewed at fixed intervals by a body that includes a judicial member, whether that is the Board once its independence is strengthened along Competition Act lines, or a separate

[27] People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301 (India).

oversight mechanism modelled on the PUCL review committee.

None of this treats the State as an ordinary Data Fiduciary, and none of it denies that sovereignty, security, and public order are legitimate grounds for some relaxation of the ordinary rules. It asks only that the relaxation be shaped the way Puttaswamy's own test requires any privacy-restricting measure to be shaped, narrow enough to fit its justification and open enough to be checked. The Rules notified in November 2025 had the opportunity to do this and did not. With the Act's core provisions still short of a year from taking full effect, and with the government reportedly considering bringing Section 17(2) into force ahead of that schedule, the window to fix this before the exemption becomes practically significant is real, but it will not stay open for long.[28]

Conclusion

Section 17(2)(a) is not, on its own terms, an unreasonable idea. Every data protection framework has to make some space for the State to act where fully consent-based processing genuinely cannot work. The problem is not that India's law makes this space, it is how it makes it, through a single, undefined, indefinitely renewable, unreviewed notification, adjudicated, if it is challenged at all, by a Board whose own selection process runs entirely through the executive. Measured against the proportionality standard the Supreme Court itself built for exactly this kind of question, the provision fails at the two limbs that matter most, narrow tailoring and a check against misuse, not because the underlying aim is illegitimate, but because nothing in the design keeps the exemption tied to that aim once granted. India has already shown, in PUCL, that it knows how to keep a security power in place while still fencing it in. Section 17(2)(a) is waiting for the same treatment, and the Act's own phased commencement gives the government and the courts a narrowing window in which to provide it.

[28] MeitY Plans to Cut Short DPDP Compliance Timeline and Notify Cross Border Restrictions for SDFs, S.S. Rana & Co. (Feb. 17, 2026), https://ssrana.in/articles/meity-plans-to-cut-short-dpdp-compliance-timeline-and-notifycross-border-restrictions-for-sdfs/.