The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

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

CROSS-BORDER DATA TRANSFER UNDER INDIA'S DIGITAL PERSONAL DATA PROTECTION ACT, 2023: EXAMINING THE BLACKLIST APPROACH

~Aviral Goyal

ABSTRACT

This article examines Section 16 of India's Digital Personal Data Protection Act, 2023, which governs cross-border data transfer through a permissive "blacklist" model rather than the restrictive "whitelist" approach found in the 2022 draft Bill that preceded it. It traces the operational detail added by Rule 15 of the Digital Personal Data Protection Rules, 2025, and highlights an overlooked fact: Section 16 does not actually come into force until approximately May 2027, meaning the current absence of any restricted jurisdiction reflects an inoperative provision rather than a considered regulatory judgment. The article situates India's approach against the European Union's adequacy-based framework under the GDPR and China's three-pathway model under the Personal Information Protection Law, and argues that the principal risk for Indian businesses lies not in the current absence of friction, but in the unreviewable executive discretion the provision will vest once it commences.

INTRODUCTION

Somewhere between two successive drafts of the same legislative idea, India's approach to cross-border data transfers quietly flipped on its head. A bill that once presumed data could not leave the country unless a foreign jurisdiction was expressly cleared for entry became, in its final enacted form, a law that presumes data can leave freely unless a jurisdiction is expressly shut out. That reversal, compressed into a single provision of the ***Digital Personal Data Protection Act, 2023***, is the subject of this article, and it deserves more scrutiny than its brevity suggests, because a rule this permissive on its face conceals a regime that has, as of this writing, never actually been tested.

THE STATUTORY TEXT: SECTION 16 AND THE LOGIC OF THE NEGATIVE LIST

Section 16(1) of the Act provides that the Central Government may, by notification, restrict the transfer of personal data by a data fiduciary for processing to such country or territory outside India as may be so notified.[1] On careful analysis, it can be observed that the framing of the provision is a negative one; it does not create a general prohibition on transfer subject to exceptions, but rather a general permission subject to exceptions. Personal data may be sent anywhere in the world by default, and the government's role is confined to identifying the specific jurisdictions to which that default permission does not extend. This is what commentators have come to call the "**blacklist**" model, and it stands in deliberate contrast to regimes that require affirmative clearance before any transfer may occur at all.

FROM WHITELIST TO BLACKLIST: A LEGISLATIVE REVERSAL

The blacklist model was not India's first instinct. The **draft Digital Personal Data Protection Bill, 2022**, which is the immediate predecessor to the enacted Act, took a completely opposite approach in its **Section 17**, by providing that cross-border transfers would be permitted only to countries or territories the Central Government chooses to notify, with no transfer permitted to any other jurisdiction in the absence of such notification.[2] Thus, the 2022 draft, in substance, adopted a whitelist approach which provides for a closed universe of approved destinations, expanding only as the government chose to add to it, with every other country in the world presumptively off-limits. Industry experts at the time of release of the draft bill were openly worried that a whitelist approach which confined data transfer to a handful of cleared jurisdictions could be crippling for a country positioning itself as a global data-processing hub, and that criticism appears to have landed.[3] By the time the Bill was enacted as the Digital Personal Data Protection Act, 2023, the government had reversed course entirely by replacing the closed whitelist system with the open blacklist system that now governs Section 16. As per the government, the reversal was a deliberate concession in the favour of the ease of doing business, trading the certainty of a pre-vetted list for the flexibility of an open default.

---

[1] The Digital Personal Data Protection Act, No. 22 of 2023, § 16(1) (India).

[2] The Digital Personal Data Protection Bill, 2022, § 17 (India) (draft, superseded).

[3] Aria Thaker, *Data Protection Bill Might Allow Data Transfers Only to Whitelisted Countries*, Media Nama (Dec. 14, 2022), https://www.medianama.com/2022/12/223 -dpdp-bill-2022-data-transfers-whitelist-countries-nama/.

RULE 15 AND THE DUAL-INSTRUMENT DESIGN

Section 16 is merely an enabling provision which says a restriction mechanism may exist without describing how that mechanism will actually operate in practice. That operational detail arrived with the Digital Personal Data Protection Rules, 2025, notified on 13 November 2025, of which Rule 15 is the specific implementing provision for cross-border transfer.[4] Rule 15 operationalizes this blacklist architecture and adds a second, narrower instrument alongside the general country-wide restriction. It provides that the government may also issue what amounts to a *special order* targeting a particular sector, entity, or category of data, without disturbing the general permissibility of transfers to the rest of that country. For instance, a restriction could be confined to the transfer of health data or children's data to a specific foreign entity, leaving every other category of transfer to that same jurisdiction untouched. This dual-instrument structure gives the government both a broad brush for systemic geopolitical concerns and a scalpel for narrower regulatory ones, echoing the blocking-order architecture India already uses under Section 69A of the Information Technology Act, 2000 for digital platforms generally.

A REGIME NOT YET ALIVE: THE STAGGERED COMMENCEMENT PROBLEM

The detail most conspicuously absent from popular commentary on Section 16 is that the provision is not actually in force yet. The notification bringing the DPDP Rules into effect activates different parts of the framework on a staggered timeline. The foundational and Board-related provisions took effect immediately, while the operational obligations bound up with Section 16 itself become effective only eighteen months after the November 2025 notification, placing the practical start date for cross-border transfer restrictions at approximately May 2027.[5] This is a materially different situation from a regime that is live but simply has not yet exercised its restrictive power. It is a regime that, as of the date of this article, cannot yet exercise that power at all. No restricted-country notification has been issued, none could lawfully be issued before the commencement date, and businesses currently structuring their cross-border data infrastructure are doing so against a provision that exists on paper but has no operative teeth for roughly another year.

---

[4] The Digital Personal Data Protection Rules, 2025, r. 15 (India) (notified Nov. 13, 2025).

[5] *India's New Cross-Border Data Transfer Framework*, K&S Partners (2026), https://ksandk.com/data - protection-and-data-privacy/indias-new-cross-border-data-transfer-framework/.

THE ROAD NOT TAKEN: GDPR'S ADEQUACY ARCHITECTURE

The European Union's General Data Protection Regulation offers the clearest structural counterpoint. Chapter V of the GDPR permits transfers of personal data outside the European Economic Area only where the recipient jurisdiction has been the subject of a formal adequacy decision by the European Commission, certifying that the jurisdiction's data protection standards are essentially equivalent to those within the Union.[6] In the absence of such an adjudication in favour of the recipient jurisdiction, a transfer may still proceed, but only through one of a defined set of alternative safeguards, for instance, Standard Contractual Clauses (SCCs) approved by the Commission, Binding Corporate Rules (BCRs) for intra-group transfers, or a handful of narrower derogations for specific situations.[7] The structural logic is the complete mirror image of Section 16. Here, a transfer is presumptively prohibited , and a fiduciary must affirmatively locate itself within a permitted category before data may lawfully leave the Union. Where India's model asks only whether a destination has been blacklisted, the GDPR model asks whether the destination, or the specific transfer mechanism used, has been affirmatively cleared. The European approach trades ease of doing business for a continuously updated, evidence-based assessment of every jurisdiction data might reach; the Indian approach trades that continuous assessment for administrative simplicity and, its critics would say, for a considerably thinner evidentiary basis before any transfer occurs.

THE MIDDLE PATH: CHINA'S THREE-PATHWAY MODEL

Between these two polar opposite approaches lies ***China's Personal Information Protection Law***, which neither maintains a whitelist of approved destinations nor provides for permissive blacklisting, but instead conditions cross-border transfer on the data exporter's own risk profile. Article 38 of the PIPL requires exporters to use one of three lawful pathways depending on the scale and sensitivity of the data involved: a mandatory security assessment conducted by the Cyberspace Administration of China for critical information infrastructure operators and for large-volume transfers, a filed standard contract for mid-tier transfers, or, as of a certification mechanism that became fully operational on 1 January 2026, third-party certification from a

[6] Regulation 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 (General Data Protection Regulation), art. 45, 2016 O.J. (L 119) 1.
[7] *Id.* art. 46.

CAC-accredited institution for exporters who fall between those thresholds.[8] China's approach is more procedurally demanding than India's in every scenario and more demanding than the GDPR's in the specific case of large-scale or sensitive transfers, since it requires an ex ante governmental security assessment rather than a self-executed contractual safeguard. Positioned against this spectrum, India's blacklist model is unambiguously the most permissive of the three major frameworks now operating among the world's largest digital economies, a fact that is either a competitive advantage or a protective gap depending on which side of the transfer one happens to sit on.

COMPLIANCE IMPLICATIONS FOR INDIAN TECH AND STARTUPS

For the moment, the practical compliance burden on Indian data fiduciaries is unusually light by comparative standards. There is no requirement to execute Standard Contractual Clauses, no Binding Corporate Rules to draft, no Transfer Impact Assessment to conduct, and no pre-clearance to seek before moving personal data to a cloud provider, a SaaS vendor, or an offshore processing centre anywhere in the world. For a start-up choosing a cloud region or a company selecting an offshore support vendor, this is a genuinely low-friction environment, and it is not difficult to see why the government's reversal from the 2022 whitelist was welcomed by industry at the time. The difficulty of this approach lies in that this low-friction environment is built on a foundation that the government can unilaterally alter, with no requirement of prior consultation, no defined criteria a jurisdiction must fail before being restricted, and no indication in either the Act or the Rules of how much notice, if any, will precede a restriction taking effect. **Section 17(2)(a)** compounds this uncertainty by exempting government agencies from most compliance obligations where processing is undertaken in the interest of national security or for the maintenance of friendly relations with foreign states, meaning that the same instrument that governs private commercial transfers sits inside a broader framework where the state's own data-handling is judged by a considerably looser standard.[9] A business that has built its cloud architecture around a particular jurisdiction, has already negotiated long-term contracts with an offshore vendor, or committed capital to a specific data-residency arrangement has no statutory assurance that the arrangement will remain lawful for the life of the contract. The absence of present-day friction is not the same

[8] Personal Information Protection Law of the People's Republic of China, art. 38 (2021); Measures for the Certification of Cross-Border Transfer of Personal Information (China) (effective Jan. 1, 2026).
[9] The Digital Personal Data Protection Act, No. 22 of 2023, § 17(2)(a) (India).

thing as the absence of future risk, and businesses planning multi-year data infrastructure would be prudent to treat the current permissive window as contingent rather than settled.

THE FALSE COMFORT OF AN EMPTY LIST

This is where the more searching critique of Section 16 belongs, and it is a critique about institutional design rather than about the text of the provision itself. An empty blacklist, particularly one that cannot yet be populated because the underlying provision has not commenced, creates an appearance of low regulatory friction that is not the same as an actual assessment that all destinations are currently safe. No jurisdiction has been evaluated and found adequate, in the way the GDPR requires evaluation before permitting transfer; jurisdictions have simply not yet been evaluated at all, in either direction. The absence of a blacklist entry is not evidence of a considered judgment that a given country's data protection standards are acceptable. At present, it is simply evidence that the government has not yet been required to look. Once the commencement date arrives and the government does begin to exercise its Section 16 power, that exercise will be almost entirely unreviewable in the ordinary sense that matters to a business trying to plan around it. The Act specifies no criteria the government must apply before restricting a jurisdiction, no consultation process, and no judicial or quasi-judicial review mechanism specific to a restriction decision, leaving affected fiduciaries to challenge such a notification, if at all, through ordinary writ jurisdiction rather than through any statutory appellate channel built into the data protection framework itself. A regime this discretionary is not necessarily worse than the GDPR's more procedurally demanding alternative, since procedural weight has its own costs in delay and compliance overhead that fall hardest on smaller players. But it is worth naming plainly what the current arrangement actually is: not a settled judgment that cross-border transfer from India is broadly safe, but a deferred judgment, parked behind a commencement date roughly a year away, resting entirely on the discretion of the executive once that date arrives.

CONCLUSION

Section 16 of the Digital Personal Data Protection Act, 2023 represents a genuine and consequential policy choice, and on the narrow question of whether India should prefer a permissive default over a restrictive one, the case for the blacklist model is a reasonable one to make. The difficulty lies not in the choice itself but in how easily its current dormancy can be mistaken for a considered verdict on safety. Businesses reading the empty list as a green light,

and journalists and commentators describing India's approach as settled and business-friendly without qualification, are both skipping over the fact that the mechanism has not yet had the chance to do anything at all. Whether India's blacklist model proves to be a durable middle ground between the GDPR's rigor and the fully open transfers of earlier decades, or simply a permissive interlude before a more assertive Rule 15 order arrives without warning sometime after May 2027, is a question this Act cannot answer on its own. It is a question only the government's first restriction notification, whenever it comes, will actually settle.