scripted

Volume 22, Issue 2, December 2025

Cross-Border Data Transfers and Data Localization Mandate under the Data Protection Regime

Khushi Malviya and Eeshaan Singh***

DOI: 10.2218/scrip.220225.150

Abstract

The present paper critiques India's approach to cross-border data transfers under the Draft Digital Personal Data Protection Rules 2025. It highlights concerns with Rule 14 and Rule 12(4), which grant the government broad discretion to impose data localization mandates, potentially restricting the transfer of specific data types regardless of the destination country's safety. This "regressive" approach could stifle innovation and create compliance hurdles for businesses, especially social media intermediaries. The paper also points out the ambiguity in defining restrictions and the lack of provisions for "onward transfers" of data, contrasting it with the more comprehensive GDPR. It advocates for a balanced framework with clear criteria for restrictions and safeguards, aligning with international best practices to ensure both national security and economic viability.

Keywords
Personal data; data localization; cross border transfers; onward transfer; social media intermediaries

* Student, Batch of 2026, The West Bengal National University of Juridical Sciences (NUJS), Kolkata, khushi221021@nujs.edu.
** Student, Batch of 2026, The West Bengal National University of Juridical Sciences (NUJS), Kolkata, eeshaan221055@nujs.edu.

1 Introduction

India's evolving stance on data localization reflects a growing emphasis on safeguarding personal data while enabling cross-border data flows. Rule 14 on cross border transfers of the DPDP Draft Rules, 2025 specifies that any entity processing personal data within India, or outside India in connection with offering goods or services to data principals in India, may transfer personal data to a foreign state or persons/entities under its control, only if it complies with restrictions imposed by the Indian Government on transferring such data.[1] Read together with Rule 12(4), this framework raises concerns regarding regulatory clarity, business certainty, and the potential impact on global data exchange. A comparative analysis with the GDPR highlights the need for greater precision in delineating permissible transfer mechanisms. Accordingly, a balanced regulatory framework is recommended, one that upholds national interests without unduly constraining India's participation in the global digital economy.

2 Regulatory Evolution of Data Localization Requirements

Data localization refers to the practice, often mandated by law or regulation, of requiring data to be physically stored or processed within the geographical boundaries of a specific jurisdiction, typically the country where the data originated or pertains to its citizens. It functions primarily by restricting the cross-border transfer of data. These restrictions can manifest in various forms, ranging from absolute prohibitions on data leaving the country to conditional requirements where data can only be transferred after meeting specific criteria,

[1] Draft Digital Personal Data Protection Rules 2025, r 14 <https://cdn.digitalindiacorporation.in/wp-content/uploads/2025/01/Draft-Digital-Personal-Data-Protection-Rules2025.pdf> accessed 15 December 2025.

such as obtaining user consent or ensuring the destination country meets local data protection standards.

India's approach to data localization has evolved significantly over time, balancing national security, economic growth, and global integration.[2] Initially, the 2018 draft Personal Data Protection Bill (PDPB), based on the Srikrishna Committee report, proposed strict localization: requiring all personal data to be mirrored in India and mandating exclusive domestic storage and processing for undefined "critical personal data."[3] The 2019 version maintained these hard rules, sparking industry concerns over costs, feasibility, and impacts on innovation and trade.[4] Over time, these rigid measures softened; the 2022 draft shifted to a "whitelist" system, allowing data transfers only to government-approved countries.[5] However, the final Digital Personal Data Protection Act (DPDPA) 2023 took a more flexible turn with a "blacklist" model permitting cross-border data transfers by default unless explicitly restricted by the government.[6]

Rule 12(4) on SDF obligations proposes that they must ensure that *specific categories* of personal data (as identified by the Central Government based on a committee's recommendation) are processed under restrictions, *including not being transferred outside India without authorization*.[7] This is a direct, albeit conditional, data localization requirement targeted specifically at SDFs for

---

[2] Ministry of Electronics and Information Technology, *White Paper of the Committee of Experts on a Data Protection Framework for India* (2017) <https://www.lakshmisri.com/Media/Uploads/Documents/White_paper_on_data_protection_in_India.pdf> accessed 15 December 2025.

[3] Committee of Experts on Data Protection Framework for India, 'A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians' (*MeitY*, 2018) <https://prsindia.org/files/bills_acts/bills_parliament/2019/Committee%20Report%20on%20Draft%20Personal%20Data%20Protection%20Bill,%202018_0.pdf> accessed 15 December 2025.

[4] Personal Data Protection Bill 2019 (India), cls 33–34.

[5] Digital Personal Data Protection Bill 2022 (India), cls 17–18.

[6] Digital Personal Data Protection Act 2023, s 16(1).

[7] Draft Digital Personal Data Protection Rules 2025 (n1) r 12(4).

certain data types which is beyond the scope of territorial/geographical blacklisting. It enhances regulatory uncertainty on part of the Government, since there are no clear criteria or processes to determine which company can be designated as SDFs. This puts the businesses at a disadvantage since they don't have sufficient notice and predictability to understand when they will have obligations as an SDF.

The DPDP Act has generally allowed personal data to flow out of the country, only restricting transfers to specific destinations the government flags as unsafe. However, new rules introduce a complication: they empower the government to create a list of *specific types* of personal data (perhaps things like health records or biometric information, though the rules aren't clear yet) that important data-handling companies or SDFs cannot send outside India *at all*, regardless of how safe the destination country is.

This approach of forcing certain *categories* of data to stay within India is considered regressive because it fragments the global data flows essential for modern innovation and business operations. Instead of facilitating smoother, albeit regulated, international data exchange (the direction many modern regulations aim for), it creates complex, costly hurdles for businesses that rely on global systems, potentially isolating parts of India's digital economy. This fails to materially improve data security and seems inconsistent with the DPDP Act's original focus on blocking transfers *to risky countries*, not blocking *specific data types* universally. Furthermore, there's a lack of clarity on how the government committee will even decide *which* data types to restrict, and open-ended terms like 'traffic data' are introduced without a clear link to the personal data protected under the Act, adding to the uncertainty and burden.[8]

[8] Ibid.

Rule 14 further reinforces this by granting the Central Government broad discretion to impose localization mandates on any data fiduciary through notifications.[9] Rule 14 could effectively function as an enabling mechanism for data localization, as restricting cross-border data transfers to an extremely limited scope would, in essence, amount to a de facto localization requirement. Instead of embedding such obligations in an ambiguous and piecemeal manner, the law should explicitly define reasonable limits on government intervention to ensure that the interests of data principals are protected while maintaining regulatory clarity.

Some degree of data localization is necessary, particularly considering enforcement, evolving geopolitical risks and the rapid advancement of emerging technologies. Retaining sensitive data within India can serve as a safeguard against foreign government surveillance and unauthorized access.

3 Comparative Analysis

The global landscape of data localization is highly fragmented, reflecting diverse national priorities and regulatory philosophies. Approaches range significantly, China and Russia enforce stringent localization mandates, prioritizing state control and security oversight. The European Union, through its General Data Protection Regulation (GDPR), employs a safeguard-based system focused on protecting data subject rights; while not explicitly mandating localization, its stringent cross-border transfer rules create significant *de facto* pressures towards keeping data within the EU/EEA.[10]

[9] Draft Digital Personal Data Protection Rules 2025 (n1) rr 12 and 14 accessed 15 December 2025.
[10] European Data Protection Board, Guidelines 05/2021 on the Interplay between the Application of Article 3 and the Provisions on International Transfers as per Chapter V of the GDPR (Version 2.0, 2023) <https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052021-interplay-between-application-article-3_en> accessed 15 December 2025.

Feature	India	EU (GDPR)	Singapore (PDPA)
Primary Approach	Permesive with "Negative List"	Restricite by Default	Accountability-Based
Adernative Mechnisn Transfer Tools	Government Blacklists	EC Adeucacy Decisions	No Formal List; APEC CBPR
Government Direct Control	Consent, Contracts	SCCs, BCRs	Contracts, BCRs
Core Philosophy	National Interest	Data Rights Protection	Organizational Accantabillity

India's approach should not be one of blanket restrictions but rather a balanced framework that ensures both national security and economic viability for businesses operating in a globalized digital ecosystem.[11] This is supported by the data regime presented under the Data Empowerment & Protection Architecture, which posits a "empowerment through data" perspective - its aim is to ensure that both citizens and businesses are equitably represented in the Indian data protection regime.[12]

4 Risks & Challenges

4.1 Impact on Social Media Intermediaries

The current law presents a bundle of interconnected unresolved issues. First, with the increasing complexity of AI and digital ecosystems, it remains unclear

[11] Organisation for Economic Co-operation and Development, 'The OECD Privacy Framework' (2013) <https://web-archive.oecd.org/pdfViewer?path=/2013-09-05/247484-oecd_privacy_framework.pdf> accessed 15 December 2025.

[12] NITI Aayog, 'Data Empowerment and Protection Architecture: A Secure Consent-Based Data Sharing Framework to Accelerate Financial Inclusion' (Draft for Discussion, August 2020) <https://www.niti.gov.in/sites/default/files/2023-03/Data-Empowerment-and-Protection-Architecture-A-Secure-Consent-Based.pdf> accessed 15 December 2025.

to what extent cross-border data transfers can be effectively regulated without stifling technological advancement. Second, there is a fundamental lack of clarity on the scope of regulation, does the law apply uniformly to all entities handling data, or are specific obligations placed on government and private entities separately? This ambiguity complicates the enforcement of data protection measures.

A particularly pressing challenge is the impact of localization mandates on social media intermediaries. If classified as SDFs, these platforms will be required to implement stringent technical and organizational measures, including local data storage, encryption, and access controls, to comply with Rules 12(4) and 14.[13] Given their global infrastructure and foreign ownership, such requirements may prove operationally complex and commercially unviable. The Rules empower the Central Government to mandate SDFs to store specific categories of personal data within India's borders, necessitating significant investment in domestic data infrastructure and operational restructuring. Additionally, restrictions on cross-border data transfers create compliance challenges for multinational companies and potential legal conflicts for social media platforms that must balance Indian regulations with their obligations under foreign legal frameworks.

4.2 Ambiguity in defining restrictions under Rule 14

The provision in Rule 14 empowering the Central Government to impose "restrictions" on cross-border data transfers without clear criteria, poses significant challenges to India's data protection framework. The absence of defined guidelines allows for discretionary and potentially arbitrary decisions,

[13] Draft Digital Personal Data Protection Rules 2025 (n1) rr 12(4) and 14.

risking inconsistent application of the law.[14]

For businesses, particularly in technology, e-commerce, and fintech sectors, this ambiguity translates into compliance challenges. This not only hinders operational efficiency but also discourages international partnerships and innovation. Moreover, the potential for misuse of these provisions for non-data protection objectives, such as advancing industrial policy or restricting foreign competition, poses significant risks to India's standing as a global digital economy. Such ambiguity could deter foreign investment, adversely affecting India's IT, fintech, and e-commerce sectors, which are heavily reliant on cross-border data flows.[15]

To address these concerns, there must be clear and objective criteria for imposing restrictions on data transfers. For instance, the criteria could assess the adequacy of data protection laws in the recipient country, the sensitivity of the data involved, and the safeguards implemented by data fiduciaries.

4.3 The "Onward Transfer" Loophole

India permits data transfers to foreign recipient countries. However, the Indian data regime lacks provisions to regulate the subsequent transfers that may occur once the data reaches the recipient country. For instance, consider a scenario where India transfers data to a legitimate state, such a transfer would fall within the ambit of the Data Protection Act. However, if that legitimate state further transfers the data for commercial or other purposes, Indian law has yet to address such onward transfers.

[14] Draft Digital Personal Data Protection Rules 2025 (n1) r 14.
[15] Draft Digital Personal Data Protection Rules 2025 (n1) r 14(b).

In contrast, major legislations like the GDPR explicitly define onward transfers under its general principles of transfers.[16] The spirit of the GDPR regarding onward transfers mirrors that of regular transfer which is to ensure that the level of protection guaranteed to data principals by the regulation is not undermined. The GDPR prescribes two methods to safeguard the rights of data principals during international data transfers. The first is ensuring that the destination country provides an adequate level of protection, comparable to that of the transferee state.[17] The second method requires the data fiduciary to implement appropriate safeguards and ensure that effective legal remedies are available to data principals.[18] To this end, the GDPR offers various legal instruments, such as standard data protection clauses, binding corporate rules, and adequacy decisions.[19] Similarly, Singapore's Personal Data Protection Act (PDPA) states that transfers are allowed if the recipient state ensures comparable protection like contracts, consent etc.[20]

India currently has a limited scope of regulation on international data transfers, at least on paper. There is a need to strengthen the measures that India must adopt to ensure the protection of data beyond its borders. The data protection regime should establish a concrete legal framework with not just mere reliance on practices that are commonly followed in business, such as adequacy measures or consent. This framework should not only safeguard data transfers but also address the unique social and economic fabric of our country. It should consider factors such as processing and storage infrastructure, the local need to

[16] GDPR, art 44.
[17] GDPR, art 45.
[18] GDPR, art 46.
[19] GDPR, arts 46–48.
[20] Personal Data Protection Act 2012 (Singapore), s 26.

boost the digital economy, and efforts to minimize the impact of data colonialism.[21]

Under the DPDP Act, data transfers are permitted to most countries, with restrictions only applying to those placed on a government-designated "negative list."[22] To build on this, there should be a clear legal mechanism for determining the threshold of protection offered and for regulating subsequent data transfers to third-party countries, with appropriate safeguards in place.

4.4 Artificial Intelligence (AI) Compliance with Localization Mandate

Emerging technologies such as AI further complicate compliance with localization mandates, as their efficacy often depends on access to large, diverse, and geographically dispersed datasets. AI models require continuous training and refinement, which is best achieved through the free flow of cross-border data. Strict localization rules may fragment these datasets, resulting in biased or less accurate outcomes, particularly in sectors like fintech, healthcare, and cybersecurity where global insights are essential. Moreover, AI service providers frequently rely on distributed cloud infrastructure, where data is processed dynamically across multiple jurisdictions. Imposing rigid storage requirements within India could therefore create operational inefficiencies, increase costs for innovators, and disincentivize global collaboration. Thus, while localization may be justified for sensitive categories of data, a blanket approach risks stifling AI innovation and undermining India's ambitions of becoming a global leader in digital technologies.

---

[21] Business Software Alliance, 'BSA Comments on India's Draft Digital Personal Data Protection Rules, 2025' (27 February 2025) <https://www.bsa.org/files/policy-filings/02272025bsadpdprules.pdf> accessed 15 December 2025.

[22] Digital Personal Data Protection Act 2023, s 16(1).

5 Recommendations

Rule 14 of the Draft DPDP Rules forms an open-ended, flexible framework for cross-border transfer by not instituting any requirements under the Act itself. The Government has a significant role as a regulator in the domain of cross-border transfers, and it is yet to be seen how they choose to occupy this position. However, certain ambiguities, as well as the possibility of overly harsh restrictions on such transfers, can cause reservations on part of commercial entities as well as the average citizen interfacing with the Act.

Rule 14 should clearly allow the transfer of personal data across borders when organizations use internationally recognized safeguards-such as standard contractual clauses, binding corporate rules, or similar legal commitments, that ensure data is protected. Restrictions on such transfers should be limited only to situations where data is being sent to countries with significant, well-documented risks to data protection, for example, countries on a government-maintained blacklist that lack privacy laws or oversight, and only if no protective commitments are in place. This approach would enable Indian businesses to operate globally and securely, align with international best practices like the GDPR, and avoid unnecessary barriers to data flows while still protecting individuals' privacy in high-risk scenarios.