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 GOVERNANCE IN THE DIGITAL AGE: EVALUATING RULE 15 OF INDIA'S DPDP RULES, 2025 AGAINST THE GDPR'S SCC FRAMEWORK

~ Ms. Aashi Lalchand Khanchandani

ABSTRACT

The Digital Personal Data Protection Rules, 2025, notified on 13 November 2025 to implement Section 16 of the DPDP Act, 2023, via Rule 15 permit cross-border personal data transfers by default and vest the Central Government with broad authority to restrict them by general or special order. This paper compares Rule 15 with the EU GDPR's adequacy decisions and, more commonly, its 2021 Standard Contractual Clauses (SCCs) under Article 46, as refined by the CJEU in Schrems. The analysis finds that while Rule 15's negative-list approach offers Indian businesses significant flexibility, it reduces legal predictability, exporter accountability, and remedy clarity for data principals, whereas the SCC framework addresses these via enforceable contractual warranties, third-party beneficiary rights, and mandatory transfer impact assessments. Drawing on the legislative history, Rule 15, Rules 13(4)-(5), Section 17(2)(a), and the post-Schrems II evolution of SCCs, this paper recommends retaining the negative-list default while introducing an optional, government-recognized contractual instrument. This would allow data exporters to demonstrate accountability when transferring data to non-blacklisted but legally uncertain jurisdictions, without fully adopting the EU's adequacy model.

Keywords: Cross-border data transfer, Digital Personal Data Protection Rules, 2025, Standard Contractual Clauses, General Data Protection Regulation, Schrems II

I. INTRODUCTION

Today, personal data crosses border as easily as goods once did at customs, but it often includes sensitive information such as financial details, health records, and biometric identifiers. If misused, these can cause harm long after the original transaction. Finding a way to regulate this flow without harming the digital economy is a major challenge in data protection law. The European Union addresses this with a system based on adequacy decisions and, when those are not available, Standard Contractual Clauses under Article 46 of the General Data Protection Regulation.[1] In contrast, India has taken a different approach: Rule 15 of the Digital Personal Data Protection Rules, 2025 allows personal data to be exported to any country by default, unless the Central Government decides to restrict transfers through a general or special order.[2]

This difference is intentional. The GDPR is used as the primary point of comparison for three reasons.

- **First**, it is still the most influential global framework for international data transfers.
- **Second**, its SCC mechanism is the primary legal route for transfers to countries without adequacy status, which is important for India, as it has never received such a determination.
- **Third**, the GDPR is the clearest example of accountability-based cross-border governance, making it a good standard for evaluating the more flexible approach of Rule 15.

These approaches show two different ways of thinking about the roles of the state, citizens, and the global data economy. In Europe, a transfer is considered illegal unless the exporter can prove that the destination country, or a contract, provides protections similar to those in the EU.[3] In India, the default is the opposite: transfers are allowed unless the government steps in to stop them. Both systems aim to balance economic openness with privacy, but they differ greatly in who carries the burden of proof, who makes decisions, and what remedies are available. This paper explores whether Rule 15, together with Section 16 of the Digital Personal Data Protection Act, 2023 ("the DPDP Act"), creates an effective and clear system for cross-border data governance. It also

[1] Regulation (EU) 2016/679, of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), art. 46, 2016 O.J. (L 119) 1 [hereinafter GDPR].
[2] Digital Personal Data Protection Rules, 2025, Rule 15, Gazette of India, pt. II, sec. 3(i) (Nov. 14, 2025) [hereinafter DPDP Rules].
[3] Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd. & Schrems, ECLI:EU:C:2020:559, ¶ 96 (July 16, 2020) [hereinafter Schrems II].

considers whether parts of the European Union's Standard Contractual Clauses ("SCC") could be used in India without changing the negative-list approach that sets it apart. It proceeds in five other parts. Part III reviews how India's approach to cross-border transfers has evolved from the 2018 Srikrishna Committee draft to the DPDP Rules, 2025, and examines Rule 15 alongside related rules and exemptions. Part IV discusses the GDPR's SCC framework, including the 2021 updates and the CJEU's decision in *Data Protection Commissioner v. Facebook Ireland Ltd. and Schrems ("Schrems II")*[4], which changed exporter obligations. Part V compares the systems in terms of versus flexi versus flexibility, accountability and remedies, and the requirement of a transfer impact assessment. Part VI suggests a reform, and Part VII concludes.

The main objective is that Rule 15's negative-list approach gives Indian data fiduciaries considerable short-term freedom, since transfers can occur without government approval. However, this freedom comes at the expense of legal certainty, accountability for exporters, and clear remedies for people whose data leaves India.

II. LITERATURE REVIEW

The regulation of cross-border data transfers is a central focus in contemporary data protection scholarship, situated at the intersection of privacy, digital trade, national sovereignty, and global digital governance. With the increasing movement of personal data across jurisdictions via cloud computing, artificial intelligence systems, and transnational digital platforms, legal scholars debate how states can maintain privacy protections without hindering the free flow of information essential for economic growth and technological advancement.

Christopher Kuner contends that international data transfer restrictions serve not only as compliance mechanisms but also as instruments for states to extend domestic privacy norms beyond their borders.[5] Similarly, ***Lee A. Bygrave*** notes that cross-border transfer rules fulfil a dual function: protecting individual privacy and acting as tools of regulatory governance within a globalized information economy.[6]

The European Union's approach has received considerable academic attention due to its foundation on the principle of *"essential equivalence,"* which requires that personal data

[4] Schrems II, supra note 3.
[5]Christopher Kuner, *Transborder Data Flows and Data Privacy Law* 3–15 (Oxford Univ. Press 2013).
[6]Lee A. Bygrave, *Data Privacy Law: An International Perspective* 173–205 (Oxford Univ. Press 2014).

transferred outside the European Economic Area be protected to a standard substantially comparable to that provided under EU law.[7] ***Orla Lynskey*** observes that the GDPR's transfer regime embodies the European Union's constitutional commitment to data protection as a fundamental right under Article 8 of the Charter of Fundamental Rights of the European Union.[8] As a result, mechanisms such as adequacy decisions and Standard Contractual Clauses ("SCCs") are intended not only to enable data transfers but also to ensure the continuity of fundamental-rights protections irrespective of the data's location.

The jurisprudential importance of this approach was highlighted by the Court of Justice of the European Union's decision in ***Data Protection Commissioner v. Facebook Ireland Ltd. and Schrems ("Schrems II").***[9] Academic commentary widely regards *Schrems II* as a transformative development in international data transfer law, as it shifted the responsibility for assessing destination-country risks from regulators to data exporters.[10] The resulting Transfer Impact Assessment ("TIA") framework obliges exporters to evaluate foreign legal systems, surveillance practices, and available remedies prior to transferring personal data abroad, thereby embedding accountability within cross-border transfer governance.[11]

Parallel scholarly debates address issues of data sovereignty and localization. ***Graham Greenleaf*** notes that heightened governmental concern over strategic data control has led many jurisdictions to implement localization requirements or transfer restrictions to preserve domestic regulatory authority.[12] In contrast, international organizations such as the Organization for Economic Co-operation and Development (OECD) and the United Nations Conference on Trade and Development (UNCTAD) caution that excessive localization measures may increase compliance costs, fragment digital markets, and hinder innovation without delivering commensurate privacy benefits. [13]

---

[7] Regulation (EU) 2016/679, art. 45, 2016 O.J. (L 119) 1.
[8]Orla Lynskey, *The Foundations of EU Data Protection Law* 207–35 (Oxford Univ. Press 2015).
[9]Case C-311/18, *Data Prot. Comm'r v. Facebook Ireland Ltd. & Schrems*, ECLI:EU:C:2020:559 (July 16, 2020).
[10] Christopher Kuner, Reality and Illusion in EU Data Transfer Regulation Post Schrems II, 11 Int'l Data Priv. L. 201 (2021).
[11]Eur. Data Prot. Bd., Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data (Version 2.0, June 18, 2021).
[12]Graham Greenleaf, *Global Data Privacy Laws 2024: Despite COVID Delays, 80% of the World Has Privacy Laws*, 181 Priv. Laws & Bus. Int'l Rep. 10 (2024).
[13]Org. for Econ. Co-operation & Dev. (OECD), *Data Free Flow with Trust and Cross-Border Data Flows* (2022); U.N. Conf. on Trade & Dev. (UNCTAD), *Digital Economy Report 2021: Cross-Border Data Flows and Development* (2021).

In the Indian context, scholarly and policy discussions on cross-border transfers have developed in tandem with successive iterations of India's data protection framework. The Report of the Committee of Experts, chaired by Justice B.N. Srikrishna, placed significant emphasis on data sovereignty concerns and recommended localization measures, such as mandatory data mirroring and stricter controls on critical personal data.[14] Subsequent legislative proposals gradually moderated this stance, culminating in the notification-based framework established in Section 16 of the Digital Personal Data Protection Act, 2023 and Rule 15 of the Digital Personal Data Protection Rules, 2025.

Indian research on cross-border data transfers has evolved alongside legislative developments. Although practitioner's commentary is extensive, doctrinal academic analysis remains limited, primarily because relevant provisions are frequently revised. Commentary on the January 2025 Draft DPDP Rules noted that the proposed framework did not establish a coherent legal infrastructure for authorizing cross-border transfers, citing the absence of a formal adequacy recognition mechanism and a lack of standardized contractual safeguards comparable to those in other jurisdictions.[15] These concerns persisted in the final notified text, as Rule 15 maintained the permissive default and broad governmental discretion found in Draft Rule 14, with minimal substantive changes apart from renumbering.[16]

A second strand of commentary places Rule 15 within the broader context of India's data governance policy. These analyses chart the progression from the Srikrishna Committee's localization-focused recommendations, through the 2019 Personal Data Protection Bill and the whitelist model in the 2022 Draft Digital Personal Data Protection Bill, to the current negative-list framework under the DPDP Act and Rules.[17] Much of this literature treats the blacklist model as an established policy choice and concentrates on its effects on business operations, compliance costs, and international digital trade, rather than on its normative adequacy as a privacy-protection

[14]Committee of Experts Under the Chairmanship of Justice B.N. Srikrishna, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* 76–90 (2018).
[15]High Hopes, Higher Hurdles: Analysis of the DPDP Act and its Draft Rules (Part I), NLS Bus. L. Rev. Forum (Aug. 5, 2025), https://forum.nls.ac.in/ijlt-blog-post/high-hopes-higher-hurdles-analysis-of-the-dpdp-act-and-its-draft-rules-part-i/ accessed on June 28, 2026.
[16]Compare Digital Personal Data Protection Rules, 2025, Rule 15, with Digital Personal Data Protection Rules, 2025 (Draft), Rule 14 (Jan. 3, 2025).
[17]Cross-Border Data Transfers and Data Localization Mandate Under the Data Protection Regime, Vidhi Ctr. for Legal Pol'y (Nov. 18, 2025), https://vidhilegalpolicy.in/blog/cross-border-data-transfers-and-data-localization-mandate-under-the-data-protection-regime/ accessed on June 28, 2026.

mechanism, and on the GDPR. These analyses emphasize that India presently lacks institutional equivalents to the GDPR's SCCs and Transfer Impact Assessment requirements and recommend introducing adequacy criteria or model contractual safeguards to enhance accountability for cross-border transfers.[18] However, such proposals generally do not address how these mechanisms could be reconciled with Section 16's notification-based structure or the policy rationale underlying Parliament's decision to adopt a negative-list approach rather than a whitelist regime.

Despite expanding literature, a significant gap persists. Existing scholarship either examines India's framework in isolation or offers broad comparisons with the GDPR, without conducting a detailed doctrinal analysis of Rule 15 and the SCC framework as developed after Schrems II. Additionally, current commentary often treats Rule 13(4)-(5)'s localization powers and Section 17(2)(a)'s exemption for state instrumentalities as peripheral compliance provisions, rather than as integral elements of India's cross-border data governance structure.

III. INDIA'S CROSS-BORDER TRANSFER REGIME

A. Legislative Evolution

India's regulatory approach to the export of personal data has undergone at least four significant changes over eight years, each reflecting a distinct assessment of the balance between data sovereignty and digital-economy growth. The Justice B.N. Srikrishna Committee's 2018 report, which informed the first draft of the Personal Data Protection Bill, recommended mandatory mirroring of all personal data within India and exclusive domestic storage and processing for an undefined category of ***"critical personal data."***[19] The Committee's rationale was primarily based on concerns regarding foreign-government access to Indian citizens' data and the strategic disadvantage of permitting data generated by India's large user base to be processed entirely outside the country's regulatory jurisdiction. The 2019 Bill largely preserved this localization framework, which led to sustained industry objections related to cost, feasibility, and competitiveness, as the requirement for local mirroring of all sensitive data entailed significant

[18] An Overview of India's DPDP Rules 2025: Key Highlights, Ampcus Cyber (Nov. 25, 2025), https://www.ampcuscyber.com/blogs/dpdp-rules/ accessed on June 28, 2026.
[19] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians 76-90 (2018).

duplicate infrastructure investment for multinational entities already operating global data centers.[20]

The 2022 draft Bill softened the earlier localization stance by introducing a ***"whitelist"*** model that permits transfers only to government-approved countries. This approach was conceptually similar to the GDPR's adequacy mechanism, although it did not ultimately persist in the enacted law.[21] The whitelist proposal would have required the Indian government to conduct country-by-country assessments prior to authorizing any transfer, a process analogous to the European Commission's adequacy-decision procedure but lacking the Commission's extensive multi-stage consultation. The DPDP Act, 2023, as enacted, replaced the whitelist with a default-permissive, government-restrictable model: Section 16(1) empowers the Central Government to restrict transfers *"by notification"* to *"such country or territory outside India as may be so notified,"* without obligating the exporting fiduciary to seek prior clearance for transfers to non-restricted destinations.[22] This transition from a whitelist to a blacklist model occurred late in the legislative process and has been partly attributed to industry concerns that a whitelist would delay market entry and impose disproportionate compliance costs on smaller enterprises lacking the resources of large multinational technology companies. Section 16(2) maintains the applicability of any other Indian law imposing stricter protection or restrictions on transfer, ensuring that sectoral localization mandates, such as the Reserve Bank of India's requirement for exclusive domestic storage of payment-system data, continue to operate alongside the DPDP framework rather than being superseded by it.[23] The transition to a blacklist architecture reflects a broader recalibration of India's digital governance strategy. Whereas earlier proposals prioritized sovereign control over data, the final DPDP framework appears to balance privacy concerns against India's ambition to remain a competitive destination for digital services, cloud computing, and cross-border innovation. This transition suggests that economic considerations increasingly influenced the design of data governance policy, moving India closer to a trade-facilitative model while preserving residual governmental control through notification powers.

[20] Personal Data Protection Bill, 2019, Bill No. 373 of 2019, cl. 33-34 (India); see also Vidhi Centre for Legal Pol'y, supra note 17.
[21] Draft Digital Personal Data Protection Bill, 2022, cl. 17 (India); Vidhi Centre for Legal Pol'y, supra note 17.
[22] Digital Personal Data Protection Act, 2023, No. 22 of 2023, § 16(1), Acts of Parliament, 2023
[23] DPDP Act, supra note 22, § 16(2); DPDPA 2023: Full Act Text with Plain-English Guide, SaralPrivacy (Apr. 30, 2026), https://saralprivacy.com/learn/dpdp-act-2023 accessed on June 28, 2026.

The Draft DPDP Rules, released for public consultation in January 2025, operationalized Section 16 through what was initially designated as Rule 14, permitting transfers subject to compliance with government-specified conditions regarding disclosure to foreign states.[24] After the consultation period, during which stakeholders submitted comments until 18 February 2025, the Central Government issued the final DPDP Rules, 2025 on 13 November 2025, renumbering the cross-border transfer provision as Rule 15 while leaving its substantive content *"largely unchanged from the draft"*.[25] The core compliance obligations under Rule 15, along with most other operative rules, take effect eighteen months from the date of notification, providing data fiduciaries with a transition period before the provision becomes enforceable. In contrast, provisions concerning the Data Protection Board took effect immediately upon notification.[26]

B. The Text and Structure of Rule 15

Rule 15 provides, in its entirety, that personal Rule 15 stipulates that personal data processed by a Data Fiduciary under the Act may be transferred outside India, provided that the Data Fiduciary complies with any requirements the Central Government may specify by general or special-order regarding disclosure to any foreign State or to any person or entity under the control of such a State.[27] Three structural features emerge from this provision.

- **First**, the default rule is permissive: no prior governmental approval, contractual safeguard, or self-assessment is required before a fiduciary may transfer data abroad.
- **Second**, the only explicit limitation pertains to disclosure to a foreign State or an entity under that State's control, which serves as a national-security and foreign-relations safeguard rather than a general data-protection standard that addresses issues such as the destination jurisdiction's surveillance laws, judicial redress mechanisms, or onward-transfer practices.
- **Third**, the provision is self-executing only in the sense that it eliminates the need for a transfer-by-transfer assessment; it does not provide a mechanism, such as a model contract

[24] Digital Personal Data Protection Rules, 2025 (Draft), Rule 14 (Jan. 3, 2025).
[25] A Closer Look at the DPDP Rules 2025, Ikigai L. (Nov. 14, 2025), https://www.ikigailaw.com/article/647/a-closer-look-at-the-dpdp-rules-2025 accessed on June 28, 2026.
[26] DPDP Rules 2025: Digital Personal Data Protection Rules Explained, BitRaser (Jan. 19, 2026), https://www.bitraser.com/article/dpdp-rules-2025.php accessed on June 28, 2026.
[27] DPDP Rules, supra note 2, Rule 15; Rule 15 DPDP Rules 2025 - Transfer of Personal Data Outside India, DPDPA.com (Mar. 19, 2026), https://www.dpdpa.com/dpdparules/rule15.html accessed on June 28, 2026.

or certification scheme, for fiduciaries to proactively demonstrate the adequacy of safeguards at the destination. Justification, as creating *"a permissive default"* under which *"there is no blanket prohibition"* on transfer and the Central Government's restrictive power operates as *"both a broad brush and a scalpel,"* capable of either blacklisting an entire jurisdiction or targeting *"transfer of health data or children's data to a named foreign entity"* through a special order.[28]

No country or category has yet been notified under Rule 15, leaving fiduciaries to operate in a state of latent, rather than actual, restriction.[29]

C. Cognate Provisions: Rule 13(4)-(5) and Section 17(2)(a)

Rule 15 does not represent the entirety of the DPDP framework's approach to cross-border data flows. Rule 13(4), which applies exclusively to entities designated as Significant Data Fiduciaries ("SDFs"), mandates that personal data specified by the Central Government, based on the recommendation of a dedicated committee, along with the associated traffic data, must not be transferred outside India under any circumstances.[30] In contrast to Rule 15's permissive default, Rule 13(4) imposes an absolute prohibition once the Central Government exercises its categorization authority, regardless of any contractual or technical safeguards offered by the SDF. Rule 13(5) establishes the advisory committee responsible for recommending such categorization, comprising officials from the Ministry of Electronics and Information Technology and, at the Central Government's discretion, officials from other ministries.[31] The inclusion of *"traffic data,"* a term not defined in either the Act or the Rules, introduces additional uncertainty, as metadata describing the flow of personal data may be significantly broader in scope than the personal data itself.[32]

Section 17(2)(a) of the DPDP Act completes the cross-border regulatory framework by exempting from the Act's operation including Section 16 and, by extension, Rule 15 any instrumentality of the State that the Central Government notifies for this purpose, provided the processing is

[28] Rule 15 DPDP Rules 2025, supra note 27.
[29] DPDP Rules 2025: India's Complete Compliance Guide, Seclore (May 26, 2026), https://www.seclore.com/fundamentals/dpdp-rules-2025-compliance-guide/ accessed on June 28, 2026.
[30] DPDP Rules, supra note 2, Rule 13(4).
[31] Id. Rule 13(5).
[32] DPDP Rules, 2025: Significant Data Fiduciaries and Data Transfers, Software Freedom L. Ctr. India (Mar. 18, 2025), https://sflc.in/dpdp-rules-2025-significant-data-fiduciaries-and-data-transfers/ accessed on June 28, 2026

undertaken in the interests of sovereignty and integrity of India, security of the State, friendly relations with foreign States, maintenance of public order, or the prevention of incitement to a cognizable offence related to these interests.[33] This provision is currently subject to constitutional challenge: a writ petition filed before the Supreme Court of India in February 2026 argues that Section 17(2), when read with Section 17(1)(c) and related provisions, creates an unreviewable surveillance exemption that violates Articles 14, 19(1)(a), and 21 of the Constitution; the matter has been referred to a larger bench for hearing.[34] The petition highlights that the cross-border framework established by Rule 15 operates within boundaries that the State itself is not required to observe when it notifies its own instrumentalities under Section 17(2)(a), a structural asymmetry not directly paralleled in the GDPR's approach to public-authority transfers.[35]

D. Interpretive Ambiguities

Three recurring ambiguities are evident in commentary on Rule 15 and its related provisions.

1. Neither the Act nor the Rules define *"traffic data"*, resulting in uncertainty as to whether the term is limited to data necessary for routing communications or extends to broader categories of metadata generated by digital services.[36]
2. The Rules do not specify the criteria that the Rule 13(5) committee must apply when recommending categories of personal data for localization, nor do they provide public consultation, judicial review, or a sunset mechanism for such recommendations.[37]
3. The most significant for this analysis, Rule 15 does not establish a procedure for the Central Government to compile, publish, or update its restricted-destination list. Practitioners expect authorities to publish a single list of prohibited jurisdictions but acknowledge that *"the law does not require the government to maintain a blacklist or whitelist at all"*.[38]

[33] DPDP Act, supra note 22, § 17(2)(a).
[34] Constitutionality of the Digital Personal Data Protection Act, 2023, Sup. Ct. Observer (Feb. 20, 2026), https://www.scobserver.in/cases/constitutionality-of-the-digital-personal-data-protection-act-2023 accessed June 28, 2026.
[35] Id
[36] Software Freedom L. Ctr. India, supra note 32
[37] DPDP Rules, supra note 2, Rule 13(5).
[38] India's DPDP Rules - Cross-Border Data Transfers Explained, MediaNama (Nov. 19, 2025), https://www.medianama.com/2025/11/223-dpdp-rules-cross-border-data-transfers/ accessed on June 28, 2026.

In the absence of such a list, the practical effect of Rule 15's restriction is negligible, and fiduciaries must structure compliance programme based on contingency rather than certainty.[39]

IV. THE GDPR'S SCC FRAMEWORK

A. Article 46 and the Hierarchy of Transfer Mechanisms

Chapter V of the GDPR establishes a strict transfer rule: personal data may be transferred to a third country only if the Regulation's level of protection is maintained.[40] Article 45 allows transfers without additional safeguards when the European Commission has adopted an adequacy decision, confirming that the destination country or a specific sector provides adequate protection. These decisions are reviewed at least every four years and may be revoked, as demonstrated by the EU-US Privacy Shield.[41] In the absence of an adequacy decision, Article 46 permits transfers provided that the controller or processor implements *"appropriate safeguards"* and ensures enforceable data subject rights and effective legal remedies.[42] Article 46(2) lists recognized safeguards, such as standard data protection clauses adopted by the Commission, approved codes of conduct, and approved certification mechanisms. Article 46(3) allows, with supervisory authority authorization, ad hoc contractual clauses and administrative arrangements between public authorities.[43] Article 47 addresses Binding Corporate Rules for intra-group transfers, which require supervisory authority approval and offer a long-term compliance solution for large multinational groups with recurring intra-group transfers.[44] India has not received an adequacy determination under this framework. Before the enactment of the DPDP Act, entities transferring data from the European Union to India relied on contractual safeguards or certification schemes to comply with Article 46.[45] According to the most recent adequacy list, only a limited number of jurisdictions, mainly in Europe and a few other developed economies, have received such recognition. As a result, SCCs serve as the primary transfer mechanism for most cross-border data flows into and out of the European Economic Area.

[39] Id
[40] Supra note 1, art. 44.
[41] Id. art. 45.
[42] Id. art. 46(1).
[43] Id. art. 46(2)-(3).
[44] Id. art. 47.
[45] Supra note 38.

B. The 2021 Modernized SCCs

The Standard Contractual Clauses under Article 46(2)(c) were revised by the European Commission's Implementing Decision of 4 June 2021. This decision replaced the three sets of clauses from the previous Data Protection Directive with a single modular instrument that accommodates four transfer scenarios: controller-to-controller, controller-to-processor, processor-to-processor, and processor-to-controller.[46] The 2021 SCCs were designed to address the implications of the CJEU's Schrems II judgment, discussed below, and therefore impose more stringent obligations than earlier versions.[47] A guarantee that the data importer has no reason to believe that the laws or practices of its jurisdiction, including any requirement to disclose data to public authorities, would prevent it from fulfilling its contractual obligations is one of the obligations imposed on the parties by the modernized clauses. They also grant data subjects, with limited exceptions, the right to invoke the clauses directly as third-party beneficiaries, allocate liability between the parties in the event of a breach of data subject rights, provide a corresponding right to compensation, and require the data importer to challenge unlawful government-access requests and inform the data exporter of any such request. [48] Additionally, the clauses align with Article 28 of the GDPR regarding processor obligations, eliminating the need for a separate data-processing agreement when a processor is involved in the transfer.[49]

C. Schrems II, Government Surveillance, and the Transfer Impact Assessment

The Court of Justice of the European Union's 16 July 2020 judgment in ***Data Protection Commissioner v. Facebook Ireland Ltd. and Schrems*** invalidated the EU–US Privacy Shield adequacy decision but upheld the validity of the SCCs as a transfer mechanism, subject to an important qualification: data exporters and importers must verify, on a case-by-case basis, whether the law or practice of the destination country undermines the effectiveness of the contractual safeguards and, where necessary, adopt supplementary measures to address those risks.[50]

---

[46] Commission Implementing Decision 2021/914 of 4 June 2021 on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries, 2021 O.J. (L 199) 31 [hereinafter 2021 SCC Decision].
[47] Just Arrived - the New Standard Contractual Clauses for International Data Transfers, White & Case LLP (June 2021), https://www.whitecase.com/insight-alert/just-arrived-new-standard-contractual-clauses-international-data-transfers accessed on June 28, 2026
[48] International Data Transfers, Eur. Data Prot. Bd., https://www.edpb.europa.eu/sme-data-protection-guide/international-data-transfers_en accessed on June 28, 2026
[49] White & Case LLP, supra note 47.
[50] *Schrems II*, supra note 4, ¶¶ 133–146.

The decision arose from concerns about United States intelligence-gathering powers, particularly under § 702 of the Foreign Intelligence Surveillance Act ("FISA") and Executive Order 12,333. The Court concluded that these surveillance mechanisms permitted public authorities to access personal data transferred from the European Union in a manner that was not limited to what was strictly necessary and proportionate, thereby failing to satisfy the standards required under Articles 7, 8, and 47 of the Charter of Fundamental Rights of the European Union.[51] The Court further observed that affected individuals lacked effective judicial remedies equivalent to those available under European law, making the Privacy Shield framework incapable of guaranteeing an essentially equivalent level of protection.[52]

Although the Court invalidated the Privacy Shield, it declined to invalidate the SCCs themselves. Instead, it held that contractual safeguards remain capable of ensuring lawful transfers if exporters undertake a substantive assessment of the destination country's legal environment and adopt supplementary protections where necessary.[53] This approach transformed the role of SCCs from a largely formal contractual mechanism to a risk-based accountability framework that requires continuous evaluation of destination-country laws and practices.

The practical manifestation of this obligation is the Transfer Impact Assessment ("TIA"), a documented, transfer-specific evaluation of the destination country's legal framework, surveillance powers, availability of judicial remedies, and the likelihood of governmental access to transferred data.[54] The assessment also requires exporters to evaluate whether supplementary technical, contractual, or organizational safeguards such as strong encryption, pseudonymization, or enhanced transparency obligations are necessary to maintain an essentially equivalent level of protection.[55]

The European Data Protection Board ("EDPB") subsequently elaborated on the requirements of this assessment through Recommendations 01/2020, transforming what had previously been an implicit due diligence expectation into a formal, auditable compliance obligation.[56] The

[51] Case C-311/18, *Data Prot. Comm'r v. Facebook Ireland Ltd. & Schrems*, ECLI:EU:C:2020:559, ¶¶ 168–185 (July 16, 2020).
[52] Id. ¶¶190–197.
[53] Id. ¶¶ 133–146.
[54] Eur. Data Prot. Bd., Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data (Version 2.0, June 18, 2021).
[55] Id. ¶¶ 48–55.
[56] Id. ¶¶ 8–28.

consequence of *Schrems II*, taken together with the 2021 SCCs, is a transfer regime in which legal certainty is achieved not through governmental pre-approval but through documented exporter accountability that remains subject to regulatory review by supervisory authorities and judicial scrutiny where necessary.[57]

D. The Accountability Logic Underlying the SCC Framework

The SCC framework is often seen as a means of transferring data through contracts, but its role is broader than that. Structurally, SCCs reflect the GDPR's wider accountability principle by making exporters responsible for transfer-related risks, not just regulators. Rather than assuming cross-border transfers are permitted unless explicitly prohibited, the GDPR requires clear justification and safeguards to protect data subjects' rights outside the European Economic Area.

This model of accountability shows that the European Union regards data protection as a fundamental right, not merely a matter of following rules. SCCs are more than contract terms; they are tools that hold exporters responsible for assessing risks in the destination country, maintaining compliance records, and ensuring data remains protected even when local laws are weaker. This framework shares regulatory duties among exporters, importers, authorities, and courts, adding several layers of oversight and enforcement.[58]

Looking at both systems, this feature sets the GDPR apart from India's Rule 15. The SCC framework expects exporters to continue assessing risks in the destination country, while Rule 15 places most risk assessment in the hands of the State through its notification powers. This difference is not just about process but about philosophy: the GDPR uses decentralized accountability by private actors under supervision, while the DPDP framework mainly relies on the government to decide which destinations are risky. Knowing this difference is key to judging if parts of the SCC model can fit into India's cross-border transfer system without changing its negative-list approach.[59]

[57] Christopher Kuner, Reality and Illusion in EU Data Transfer Regulation Post-Schrems II, 11 Int'l Data Priv. L. 201, 203–10 (2021).
[58] Orla Lynskey, *The Foundations of EU Data Protection Law* 207–35 (Oxford Univ. Press 2015).
[59] Lee A. Bygrave, *Data Privacy Law: An International Perspective* 173–205 (Oxford Univ. Press 2014).

V. COMPARATIVE ANALYSIS

A. Negative-List vs Adequacy-List: Predictability vs Flexibility

Under Rule 15, the State is responsible for issuing a restriction before a transfer becomes unlawful. Until such a restriction is announced, fiduciaries can send data to any country, even if that country has weak data-protection laws, without having to do their own risk assessment.[60] Under the GDPR, the responsibility falls on the exporter, who must either rely on a Commission adequacy decision or check independently, using the SCCs and a TIA, that the destination country's laws do not weaken the contractual safeguards.[61] This contrast makes the Indian model more permissive in the short term: a fiduciary can send data to a country with limited privacy protections without violating Rule 15, if the Central Government has not specifically restricted that country. In contrast, the European model is more protective, but it requires ongoing compliance checks for every cross-border transfer, regardless of the destination's reputation for data protection.

Under the GDPR's SCCs, a fiduciary can demonstrate a specific contract, a documented risk assessment, and guidance from the EDPB and supervisory authorities on the due diligence required at the time of transfer.[62] Under Rule 15, a fiduciary can only point to the fact that, as of now, there is no government notification against a particular country. This makes the DPDP model less predictable: it could change at any time, in any country, without warning or a set transition period for transfers already underway.[63] Commentators note that businesses are being told to include contract clauses such as *subject to DPDP Rules for notification on permitted countries* because there is no published list to guide long-term data-sharing plans. The negative-list approach offers more flexibility now, but less certainty for contracts intended to last beyond the current compliance window or any future government notification.[64]

B. Accountability and Remedies

The SCCs' third-party beneficiary mechanism allows a data subject to enforce the clauses directly against the data importer, even though the data subject is not a party to the contract between

[60] DPDP Rules, supra note 2, Rule 15.
[61] GDPR, supra note 1, art. 46; Schrems II, supra note 3, ¶ 134.
[62] Eur. Data Prot. Bd., supra note 48.
[63] Rule 15 DPDP Rules 2025, supra note 27.
[64] DPDP Act vs GDPR: Key Differences for Indian Companies (2026 Complete Comparison), Tranquility Cybersecurity (Mar. 27, 2026), https://www.tcsa.in/resources/dpdp-vs-gdpr-comparison-guide accessed on June 28, 2026

exporter and importer.[65] This mechanism, combined with the SCCs' express allocation of liability and right to compensation, gives an EU data subject whose data has been transferred abroad a contractual avenue of redress that operates independently of, and in addition to, any complaint mechanism before a supervisory authority.[66] Rule 15 supplies no equivalent. A data principal whose personal data is transferred from India to a jurisdiction that subsequently misuses it has no contractual instrument to invoke against the foreign recipient; her only recourse lies in a grievance against the Indian Data Fiduciary under Rule 14's grievance-redressal procedure and, ultimately, a complaint to the Data Protection Board of India.[67] The Data Protection Board is *'an adjudicatory body modelled more as a quasi-judicial tribunal'* without the own-initiative investigative powers exercised by European supervisory authorities such as the Irish Data Protection Commission, the practical avenues for a data principal to learn that her data has been transferred abroad, let alone misused there, remain limited to self-disclosure by the fiduciary, a security incident, or detection through a mandatory Data Protection Impact Assessment applicable only to SDFs.[68]

C. The Absence of a TIA-Equivalent Under the DPDP Rules

The DPDP Rules do not require fiduciaries to check, for each transfer, whether the destination country's laws might put personal data at risk once it leaves India. The GDPR, through its TIA requirement, makes exporters look closely at the legal system of the destination country before transferring data, even though this can be a heavy burden in practice.[69] Instead, the Central Government holds all the power to issue notifications, and it can do so only after the fact and without explaining its methods.[70] All responsibility for assessment is held by the government, and this power has not yet been used, India's cross-border safeguards depend entirely on whether the government decides to act in the future. This kind of regulatory inaction does not exist in the EU's system, where adequacy and SCC rules are always in effect[71]

[65] 2021 SCC Decision, supra note 46, cl. 3.
[66] Eur. Data Prot. Bd., supra note 48.
[67] DPDP Rules, supra note 2, Rule 14.
[68] DPDP Act vs GDPR: The Side-by-Side Comparison India's DPOs Actually Need, CreativeCyber (Apr. 29, 2026), https://creativecyber.in/resources/dpdp-act-vs-gdpr-india/ accessed on June 28, 2026
[69] Eur. Data Prot. Bd., supra note 48.
[70] DPDP Rules, supra note 2, Rule 15.
[71] Tranquility Cybersecurity, supra note 64.

D. Enforcement Architecture and the Localization Carve-Out

Another key difference is how each system handles data that is too sensitive to be exported freely. The GDPR addresses this in Article 9, which lists special categories of personal data. These categories still follow the usual Chapter V transfer rules but processing them requires a stricter legal basis. The transfer process itself does not change based on the data category.[72] In contrast, Rule 13(4) creates a separate and absolute ban on transferring certain types of personal and traffic data, as decided by the Central Government. This ban only applies to SDFs and is separate from Rule 15's more flexible approach.[73] Regular fiduciaries follow Rule 15's negative list, while SDFs may face strict localization for certain data categories. The Central Government decides this classification based on broad criteria like 'the volume and sensitivity of personal data processed and other unspecified risk factors.[74] The GDPR's enforcement rules, on the other hand, apply the same way to all controllers and processors within its scope, with the level of strictness based on the data category, not the size or type of entity. This makes the GDPR's system more predictable, even if it is less focused on specific risks. For comparison, an Indian fiduciary's cross-border risk cannot be judged by Rule 15 alone; it also depends on a separate, largely opaque government process that the GDPR does not require.

E. Constitutional Philosophy and Regulatory Design

The divergence between Rule 15 and the SCC framework ultimately reflects a deeper constitutional and regulatory distinction between the European Union and India. The GDPR's transfer regime is rooted in the European conception of data protection as a fundamental right protected under Articles 7 and 8 of the Charter of Fundamental Rights of the European Union. Consequently, cross-border transfer mechanisms are designed primarily to ensure continuity of rights protection irrespective of the geographical location of processing. The SCCs, adequacy decisions, and Transfer Impact Assessments therefore function not merely as compliance mechanisms but as instruments through which fundamental-rights guarantees are projected beyond the territorial boundaries of the European Economic Area.[75]

[72] GDPR, supra note 1, art. 9.
[73] DPDP Rules, supra note 2, Rule 13(4).
[74] DPDP Act, supra note 12, § 10.
[75] Supra note 58

India's framework originates from a different constitutional context. Although the Supreme Court of India recognized privacy as a fundamental right in ***Justice K.S. Puttaswamy (Retd.) v. Union of India,*** the DPDP Act adopts a governance-oriented model that seeks to balance privacy protection against developmental, administrative, and economic considerations.[76] The resulting architecture reflects a greater degree of trust in governmental discretion and policy flexibility than is evident in the GDPR. Rule 15 therefore prioritizes regulatory agility and economic interoperability while reserving the State with the authority to intervene where national interests require restriction of data flows.

The GDPR externalizes accountability to exporters and private actors operating under regulatory supervision, whereas the DPDP framework centralizes responsibility within governmental decision-making. Any attempt to transplant SCC-style safeguards into India must therefore account not only for differences in institutional design but also for the constitutional values that each framework seeks to advance.

VI. CRITIQUE AND RECOMMENDATIONS

India does not need to abandon the negative-list approach Parliament chose instead of the whitelist model in the 2022 draft Bill.[77] That approach has real benefits for a large, export-focused digital economy like India's. It avoids the long political process needed for adequacy decisions and does not tie routine commercial transfers to another country's diplomatic relationship with India.[78] India still has several reform options.

- One is to adopt a formal adequacy framework, such as Article 45 of the GDPR, which would allow transfers only to countries that meet specified legal standards.
- Another is to require Transfer Impact Assessments for certain high-risk transfers.
- A third option is to use approved certification systems or sector-specific transfer rules.

While these models would improve accountability, they would also raise compliance costs and could reduce the flexibility that Parliament sought to preserve under Section 16's negative-list system. In this context, an optional contractual tool is a more balanced reform. It would improve

[76] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India).
[77] Draft Digital Personal Data Protection Bill, 2022, cl. 17 (India).
[78] Vidhi Centre for Legal Pol'y, supra note 7.

accountability without changing the basic structure set by lawmakers. The proposal here is to add, not replace: introduce an optional, government-recognized contract that any fiduciary can use when sending data to a country that is not blacklisted under Rule 15 but has an uncertain or weak data-protection system. This contract could include three features from the 2021 SCCs, but without bringing in the full GDPR adequacy system.

- **First**, it could include a standard warranty clause, such as the SCCs' importer warranty regarding government access laws. This would require the foreign recipient to confirm that local law would not stop them from meeting their data-protection promises, putting some responsibility on the party that knows the local laws best.[79]
- **Second**, it could allow the Indian data principal to enforce certain contract terms directly against the foreign recipient. This would give a way to seek remedies that the current DPDP framework does not offer, and it would not need a new regulator.[80]
- **Third**, it could require a simple, proportionate transfer assessment based on the amount and sensitivity of the data, instead of copying the full GDPR TIA. This would make the contract's purpose clearer: improve accountability through a lighter-touch transfer check, not a full adequacy regime. It would encourage fiduciaries to consider risks in the destination country before transferring data, rather than relying only on the Government's notification of power.

It is important to note that these three features would not change Rule 15's default rule. Fiduciaries who do not want to use the optional contract could still transfer data to any country not on the restricted list, just as Rule 15 allows now. The contract would serve as a safe harbor, demonstrating accountability and good faith in the event of a dispute, breach, or Data Protection Board review, but it would not be required for transfers. This approach also deals with the issue in Section 17(2)(a): since the contract would only apply to fiduciaries who choose to use it, the separate constitutional question about the State's exemption from Section 16 can be settled in court, not by new rules.[81] Since the Rule 13(5) committee already reviews data-category risks for SDFs, it could also publish and update the model's contract, so there would be no need for a new regulator.[82]

[79] 2021 SCC Decision, supra note 36, cl. 14.
[80] Id. cl. 3.
[81] Sup. Ct. Observer, supra note 24.
[82] DPDP Rules, supra note 2, Rule 13(5).

CONCLUSION

Rule 15 of the DPDP Rules, 2025, adopts a clear policy stance by employing a negative-list model that enhances flexibility for India's data-driven economy, while permitting State intervention if cross-border data transfers pose risks to national security or foreign relations. Compared with the GDPR's Standard Contractual Clauses (SCC) framework, Rule 15 offers less legal certainty, reduced accountability for data exporters, and fewer remedies for individuals whose data is transferred outside India. The SCCs, particularly following Schrems II, demonstrate that a system can require exporters to conduct risk assessments through enforceable contracts and ongoing documentation, without compromising flexibility. SCCs serve as a safeguard within a regime that still facilitates transfers when adequacy is recognized. India need not choose exclusively between the flexibility of Rule 15 and the accountability of the GDPR. An optional, narrowly tailored contract, approved by the Central Government and overseen by the Rule 13(5) committee, could incorporate many of the protections offered by SCCs while maintaining India's adaptable approach to cross-border data transfers.

A broader comparison between Rule 15 and the SCC framework underscores the ongoing global debate over the balance among data sovereignty, economic integration, and privacy. As digital trade increasingly depends on seamless cross-border data flows, regulators must determine the appropriate allocation of risk management responsibilities. India currently relies on government decisions implemented through a notification system. The evolution of India's cross-border data transfer regulations will serve as a significant case study in assessing whether enhanced accountability can be achieved without compromising the flexibility considered essential for a rapidly expanding digital economy.