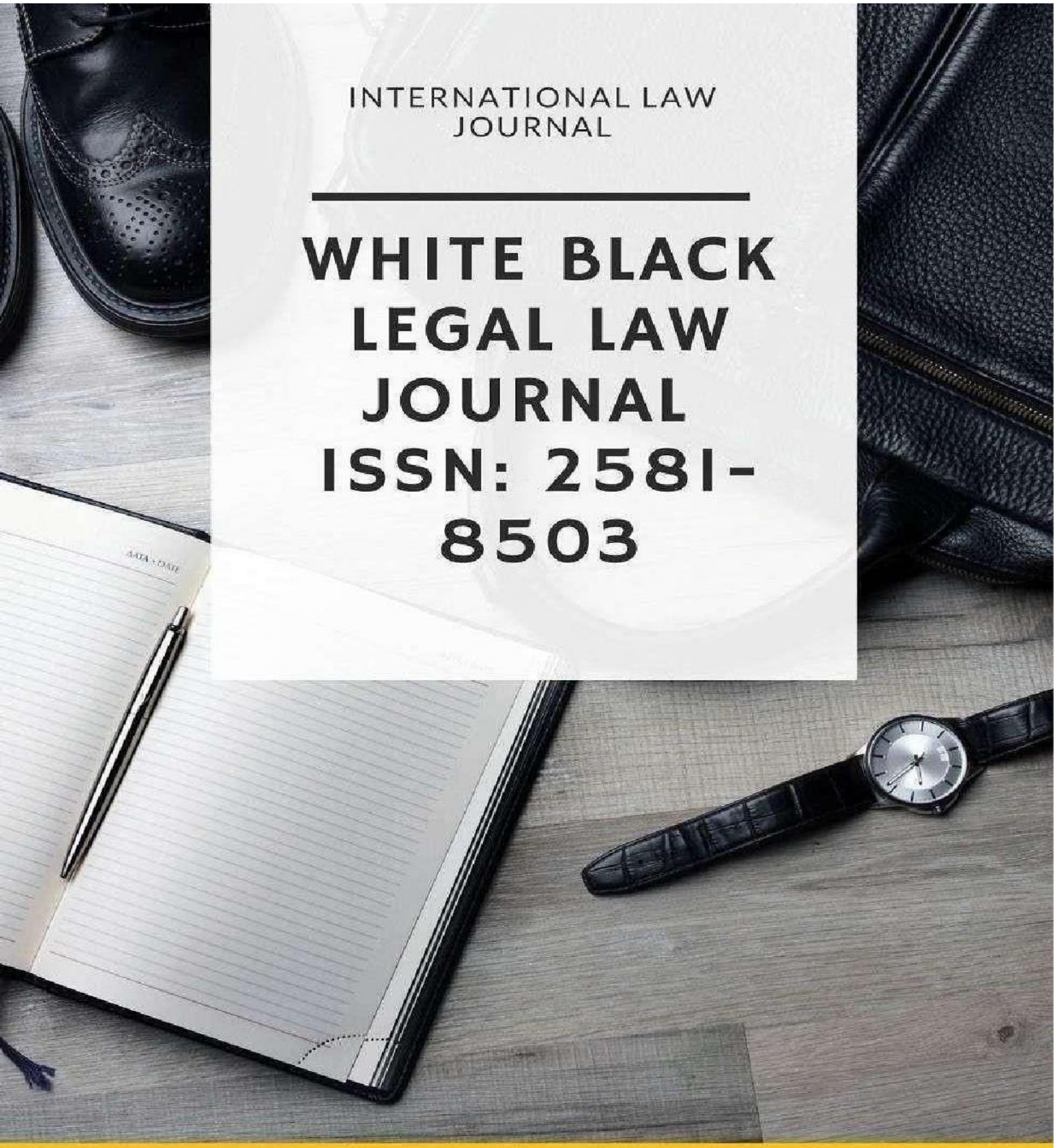

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

www.whiteblacklegal.co.in
Volume 3 Issue 8 | June 2026 ISSN: 2581-8503

CROSS-BORDER DATA TRANSFERS, DATA LOCALIZATION AND DIGITAL TRADE: A COMPARATIVE STUDY OF INDIA'S DPDP ACT, GDPR AND INTERNATIONAL TRADE LAW

AUTHORED BY - PRAVEEN CHAUDHARY

Abstract

Cross-border data transfers have become a decisive legal question for privacy protection and digital trade. Cloud computing, platform services, artificial intelligence, financial technology and outsourcing depend upon the movement of personal data across borders, while States increasingly claim regulatory authority over data for privacy, security, economic and sovereignty reasons. This paper undertakes a doctrinal and comparative analysis of India's Digital Personal Data Protection Act, 2023, the Digital Personal Data Protection Rules, 2025, the European Union's General Data Protection Regulation and the relevant principles of international trade law. It argues that India has adopted a flexible, executive-notification model that permits transfers unless restricted, whereas the EU adopts a rights-based transfer architecture based on adequacy, appropriate safeguards and limited derogations. The EU model is more procedurally detailed and judicially supervised, particularly after Schrems I and Schrems II. India's model is commercially attractive because it avoids general data localization, but it presently lacks adequate statutory criteria for country restrictions, transfer impact assessment and independent review. The paper further argues that localization measures may operate as trade barriers under the General Agreement on Trade in Services, although privacy can justify restrictions under Article XIV if measures are necessary, proportionate and non-discriminatory. The paper concludes with recommendations for India to develop transparent transfer criteria, standard contractual clauses, sectoral harmonisation, independent oversight and trusted data-flow arrangements with the EU and other partners.

Keywords: Cross-border data transfer; data localization; DPDP Act; GDPR; digital trade; GATS; WTO; adequacy; privacy; India-EU comparison.

I. Introduction

The legal governance of data has moved from a specialised privacy concern to a central question of economic policy, constitutional law and international trade. In the digital economy, personal data is rarely confined within one territory. A routine online purchase may involve an Indian consumer, a cloud server in Singapore, payment processing by a multinational network, fraud monitoring in Europe, analytics in the United States and customer support from another jurisdiction. The technical architecture of digital services is therefore transnational even where the user experience appears local. The legal challenge is that personal data is both a resource for trade and a medium through which human dignity, autonomy and decisional freedom may be affected. India's Digital Personal Data Protection Act, 2023 reflects this duality by recognising both the right of individuals to protect their personal data and the need to process it for lawful purposes.[1]

The Indian constitutional setting makes this problem especially important. In Justice K.S. Puttaswamy (Retd.) v. Union of India, the Supreme Court of India recognised privacy as a fundamental right and treated informational privacy as part of personal liberty and dignity.[2] That recognition places data protection beyond ordinary administrative policy. It demands that rules on collection, processing, retention and transfer of personal data be assessed by constitutional standards of legality, legitimate aim, necessity, proportionality and safeguards. The same issue is visible internationally. Privacy is protected under Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights, both of which prohibit arbitrary interference with privacy, family, home and correspondence.[3] The United Nations General Assembly has repeatedly recognised the right to privacy in the digital age, emphasising the risks created by surveillance, interception and data collection in contemporary technology environments.[4]

Yet, a privacy-only account is incomplete. Data transfers are also a condition for participation in digital trade. Indian information technology, business process management, financial technology, online education, e-commerce and cloud service sectors depend on lawful

[1] The Digital Personal Data Protection Act, 2023, No. 22 of 2023, long title, India Code, available at: https://www.indiacode.nic.in/bitstream/123456789/22037/1/a2023-22.pdf (last visited on 22 June 2026).
[2] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
[3] Universal Declaration of Human Rights, 1948, art. 12; International Covenant on Civil and Political Rights, 1966, art. 17.
[4] UN General Assembly, The Right to Privacy in the Digital Age, A/RES/79/175, adopted on 17 December 2024, available at: https://digitallibrary.un.org/record/4071978 (last visited on 22 June 2026).

access to global data infrastructure. Excessively strict localization may raise costs, reduce competitiveness and discourage innovation. Conversely, unrestricted transfers may expose individuals to foreign surveillance, weak enforcement and commercial misuse. The regulatory question is therefore not whether data should be free or locked within territory, but how data may move under conditions that preserve rights, legal certainty and trust.

This paper examines this question through a comparative study of India's DPDP framework, the European Union's GDPR transfer regime and international trade law. The comparison with the EU is particularly valuable because the GDPR is the most developed model of rights-based cross-border data transfer governance. It does not impose an absolute territorial lock on data; instead, it permits transfers through adequacy decisions, appropriate safeguards, binding corporate rules, standard contractual clauses and narrowly framed derogations. By contrast, the DPDP Act follows a more permissive approach: personal data may be transferred unless the Central Government restricts transfer to a notified country or territory. The DPDP Rules, 2025 add a special restriction relating to making personal data available to foreign States or entities under their control. This makes the Indian approach flexible but heavily dependent upon executive specification.

The paper advances three arguments. First, India's framework is pro-digital-trade in form because it rejects general localization, but its executive-driven architecture requires greater transparency to protect privacy and legal certainty. Secondly, the EU model demonstrates that a transfer regime can facilitate trade while insisting on enforceable rights and public-authority safeguards. Thirdly, international trade law does not prohibit privacy regulation, but it requires that privacy-related data restrictions be necessary, proportionate and not applied as disguised protectionism. India can therefore retain policy space while adopting safeguards that make its system constitutionally defensible and internationally credible.

II. Research Problem, Scope and Methodology

The research problem is situated at the intersection of three fields: privacy law, digital trade and public international economic law. Cross-border data transfer rules may be framed as privacy safeguards, national security tools, industrial policy, trade restrictions or jurisdictional control mechanisms. This multiplicity produces conceptual confusion. For example, a measure requiring payment data to be stored in India may be defended as necessary for regulatory supervision, but the same measure may also increase compliance costs for foreign suppliers. A

transfer restriction may protect data principals from weak legal systems abroad, but it may also be used to favour local data-centre businesses or domestic digital firms. A proper legal analysis must therefore separate rights-protective measures from protectionist measures.

The scope of this paper is limited to personal data and digital personal data. It does not examine non-personal data governance, competition law, cybersecurity law in detail, taxation of digital services or artificial intelligence regulation except where these are directly relevant to data transfers. The Indian part focuses on the DPDP Act and the DPDP Rules, with brief attention to sectoral localization. The EU part focuses on the GDPR, especially Chapter V. The trade law part focuses on the General Agreement on Trade in Services and the WTO e-commerce context. Preferential trade agreements are used only illustratively and not as the central doctrinal foundation.

The methodology is doctrinal and comparative. The doctrinal component analyses statutes, rules, treaty provisions, judicial decisions and official materials. The comparative component identifies similarities and differences between India and the EU on transfer architecture, institutional design, safeguards, enforcement and trade implications. The paper also uses selected secondary scholarship to understand the economic and regulatory effects of localization. It does not make empirical claims about the precise cost of Indian or EU compliance; rather, it evaluates legal structure and normative coherence.

III. Conceptual Framework: Transfer, Localization and Trust

A cross-border data transfer occurs when personal data is transmitted, accessed, stored, mirrored or otherwise made available beyond the territorial jurisdiction where it is collected or initially processed. In contemporary cloud systems, transfer does not always require a simple physical movement from one server to another. Remote access by a foreign processor, disaster recovery backups, global customer support, software maintenance and analytics pipelines may all create cross-border availability. Legal systems therefore regulate not only physical storage location but also the possibility of access and processing outside the originating jurisdiction.

Data localization is narrower but politically more visible. It requires some data to be stored or processed within the territory of a State. Localization may be hard localization, under which data cannot leave the country; soft localization, under which a local copy must be maintained; conditional transfer, under which export is allowed only after approval; or sectoral localization,

under which only specific categories such as payment data, health data or critical infrastructure data are subject to local storage. Scholars have described localization as a form of data nationalism when territorial control becomes an end in itself rather than a means of protecting individuals.[5] Other scholarship argues that data localization can become a non-tariff barrier in digitally enabled services when it increases compliance burdens without a demonstrated rights benefit.[6]

The distinction between data protection and data protectionism is central. Data protection is directed toward lawful processing, transparency, security, purpose limitation, rights of individuals and remedies. Data protectionism uses privacy or security language to restrict foreign competition or to mandate domestic infrastructure without adequate justification. The two may overlap in practice. For example, a State may have genuine law-enforcement concerns but adopt overbroad localization that harms trade more than necessary. A rigorous legal framework should therefore ask whether the measure is connected to a legitimate privacy or security aim, whether less restrictive alternatives exist, whether the measure is transparent and whether it is applied consistently.

Trust is the bridge between privacy and trade. Businesses require predictable transfer rules; individuals require assurance that their data will remain protected after transfer; governments require access to information for lawful regulatory purposes; and trading partners require that domestic regulation does not become disguised discrimination. The EU's GDPR expresses this trust logic through adequacy and safeguards. India's DPDP Act expresses it through a general permission to transfer, combined with governmental power to restrict and specify requirements. Both systems reject the idea that location alone solves privacy. The quality of law, enforceability of rights and control over public authority access are more important than mere territorial storage.

IV. India's DPDP Framework and Cross-Border Transfers

The DPDP Act applies to the processing of digital personal data within India and also to processing outside India if such processing is in connection with any activity related to offering

[5] Anupam Chander and Uyen P. Le, 'Data Nationalism', 64 Emory Law Journal 677 (2015).
[6] Neha Mishra, 'Data Localization Laws in a Digital World: Data Protection or Data Protectionism?', The Public Sphere Journal 2 (2016), available at: https://psj.lse.ac.uk/articles/45/files/submission/proof/45-1-87-1-10-20190813.pdf (last visited on 22 June 2026).

goods or services to data principals within India.[7] This extraterritorial feature is significant. It means that a foreign platform or service provider targeting Indian users may be subject to Indian data protection obligations even when processing occurs abroad. The Act is therefore not purely territorial; it combines domestic regulation with a market-facing jurisdictional trigger. However, unlike the GDPR, the Indian statute is confined to digital personal data and to non-digital personal data once digitised.

The substantive architecture of the DPDP Act is built around lawful processing for specified purposes, consent and certain legitimate uses.[8] Data fiduciaries are subject to general obligations relating to security safeguards, breach notification, grievance redressal and erasure when retention is no longer necessary. Significant Data Fiduciaries may be subject to additional obligations, including data protection impact assessment and audits.[9] In this respect, India adopts a risk-sensitive structure, though its risk vocabulary is less developed than that of the GDPR.

Section 16 is the central transfer provision. It empowers the Central Government, by notification, to restrict the transfer of personal data by a Data Fiduciary for processing to any country or territory outside India that is notified by the Government.[10] This is a negative-list model. It does not require prior approval for every transfer and does not prescribe that personal data must ordinarily remain in India. Instead, the default position is that transfer is permissible unless the Government identifies a country or territory for restriction. Section 16(2) preserves other Indian laws that provide a higher degree of protection or restriction for particular data, data fiduciaries or classes of data fiduciaries.[11]

The DPDP Rules, 2025 are important for two reasons. First, the Rules prescribe phased commencement. Rules 1, 2 and 17 to 21 came into force upon publication in the Official Gazette; Rule 4 is to come into force one year after publication; and Rules 3, 5 to 16, 22 and 23 are to come into force eighteen months after publication.[12] Secondly, Rule 15 clarifies that

[7] The Digital Personal Data Protection Act, 2023, ss. 2, 3 and 4.
[8] Id., ss. 5, 6, 7 and 8.
[9] Id., s. 10.
[10] Id., s. 16.
[11] The Digital Personal Data Protection Act, 2023, s. 16(2).
[12] The Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), r. 1, Gazette of India, 13 November 2025, available at: https://www.meity.gov.in/static/uploads/2025/11/53450e6e5dc0bfa85ebd78686cadad39.pdf (last visited on 22 June 2026).

personal data processed by a Data Fiduciary may be transferred outside India, subject to the restriction that the Data Fiduciary must meet requirements specified by the Central Government by general or special order where such personal data is made available to a foreign State, or to a person, entity or agency under the control of such State.[13] This is not an EU-style adequacy clause; it is a foreign-State-access control clause.

Rule 13(4) introduces a more localized obligation for Significant Data Fiduciaries. It requires such fiduciaries to ensure that personal data specified by the Central Government, on the recommendation of a committee, is processed subject to the restriction that the personal data and traffic data pertaining to its flow is not transferred outside India.[14] This provision creates a targeted localization possibility, but only for specified personal data and specified fiduciaries. It therefore sits between general transfer permission and sectoral localization.

India's approach has advantages. It reduces immediate compliance burdens for digital businesses, especially start-ups and Indian service exporters. It also allows the Government to respond to geopolitical or security concerns without imposing economy-wide localization. However, it has weaknesses. The statute does not set out detailed criteria for notifying a restricted country. It does not state whether the Government must consider the recipient jurisdiction's privacy law, surveillance law, independent regulator, judicial remedies, onward transfer protections or international commitments. Nor does it provide a statutory mechanism similar to standard contractual clauses, binding corporate rules or certification. This creates uncertainty for businesses and data principals.

The DPDP framework must also be read with sectoral rules. The Reserve Bank of India's payment-data storage directive, for example, requires payment system providers to ensure that the entire data relating to payment systems operated by them is stored in India, and the RBI's FAQs clarify the scope of that requirement for authorised payment system providers and banks.[15] Sectoral localization may continue because section 16(2) preserves laws imposing higher restrictions. The result is a layered Indian model: general DPDP transfer permission, executive power to restrict, possible localization for Significant Data Fiduciaries, and separate

[13] Id., r. 15.
[14] Id., r. 13(4).
[15] Reserve Bank of India, Storage of Payment System Data, DPSS.CO.OD.No.2785/06.08.005/2017-18, 6 April 2018; Reserve Bank of India, FAQs on Storage of Payment System Data, 26 June 2019, available at: https://www.rbi.org.in/commonman/english/scripts/FAQs.aspx?Id=2995 (last visited on 22 June 2026).

sectoral storage rules.

From a constitutional perspective, the strongest criticism is not that India permits data exports. Permitting data exports may be consistent with digital trade and with the practical architecture of the internet. The deeper concern is that the conditions under which transfer may be restricted or allowed are insufficiently elaborated. Puttaswamy requires that privacy-affecting State action be backed by legality, necessity and proportionality.[16] A transfer restriction that is transparent and risk-based can satisfy this standard. A restriction based on vague or unpublished criteria may not. Similarly, a permissive transfer regime without safeguards against foreign public authority access may fail to protect informational privacy in practice.

V. The European Union Model under the GDPR

The EU model begins from a different constitutional premise. Data protection is expressly recognised as a fundamental right in Article 8 of the Charter of Fundamental Rights and Article 16 of the Treaty on the Functioning of the European Union. The GDPR itself records that the protection of natural persons in relation to the processing of personal data is a fundamental right.[17] At the same time, the GDPR is also an internal market instrument. Article 1 states that the Regulation lays down rules for protection of natural persons and rules relating to the free movement of personal data.[18] Thus, the GDPR does not oppose privacy and data flows; it attempts to harmonise privacy protection to enable lawful flows.

The GDPR has an extraterritorial dimension. Article 3 applies to processing in the context of activities of an establishment in the Union, regardless of where processing takes place. It also applies to controllers or processors not established in the Union when processing relates to offering goods or services to data subjects in the Union or monitoring their behaviour within the Union.[19] This is broader and more detailed than the Indian trigger. It makes the GDPR a global compliance standard for many businesses that interact with EU data subjects.

[16] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1; see also The Digital Personal Data Protection Act, 2023, long title.
[17] Id., recital 1; Charter of Fundamental Rights of the European Union, art. 8; Treaty on the Functioning of the European Union, art. 16.
[18] Regulation (EU) 2016/679, art. 1.
[19] Id., art. 3.

Chapter V regulates transfers to third countries and international organisations. Article 44 lays down the general principle that any transfer of personal data undergoing processing or intended for processing after transfer may take place only if the conditions of Chapter V are complied with, including for onward transfers.[20] This is the opposite of India's negative-list model. The EU starts with a compliance condition: data may leave the EU only through an accepted transfer route.

The first and most privileged route is adequacy under Article 45. The European Commission may decide that a third country, territory, sector or international organisation ensures an adequate level of protection. If such a decision exists, personal data may be transferred without specific authorisation.[21] Adequacy is not identity. A third country does not need to copy the GDPR word for word; it must provide a level of protection essentially equivalent to EU law. The assessment includes rule of law, human rights, relevant legislation, public security, defence, national security, criminal law, access by public authorities, independent supervision and effective judicial redress. Adequacy therefore functions as a legal gateway for trusted data flows.

Where there is no adequacy decision, Article 46 permits transfer through appropriate safeguards, provided enforceable data subject rights and effective legal remedies are available.[22] These safeguards include legally binding instruments between public authorities, binding corporate rules, standard contractual clauses adopted by the Commission, approved codes of conduct and approved certification mechanisms. Binding corporate rules under Article 47 are particularly important for corporate groups engaged in intra-group transfers.[23] Standard contractual clauses are the most common tool because they create pre-approved contractual obligations for exporters and importers.

Article 49 provides derogations for specific situations, such as explicit consent after being informed of risks, necessity for performance of a contract, important reasons of public interest, legal claims and vital interests.[24] These derogations are narrow. They are not meant to become routine transfer mechanisms for large-scale, repetitive processing. The structure of Chapter V

[20] Id., art. 44.
[21] Id., art. 45.
[22] Id., art. 46.
[23] Id., art. 47.
[24] Id., art. 49.

therefore creates a hierarchy: adequacy first, safeguards second and derogations only exceptionally.

The European Commission's own public explanation confirms that EU data protection legislation includes safeguards for transfers to third countries, including adequacy decisions, standard contractual clauses and binding corporate rules.[25] The Commission has also adopted modern standard contractual clauses through Implementing Decision (EU) 2021/914.[26] These clauses respond to complex modern transfer chains by providing modular clauses for controller-to-controller, controller-to-processor, processor-to-processor and processor-to-controller transfers.

The EU model is judicially supervised. In Schrems I, the Court of Justice invalidated the Safe Harbour adequacy decision for EU-US transfers and emphasised that the existence of a Commission decision does not remove the power of supervisory authorities to examine individual complaints.[27] In Schrems II, the Court invalidated the EU-US Privacy Shield adequacy decision but upheld standard contractual clauses in principle, subject to the requirement that exporters and authorities assess whether the law of the recipient country allows compliance in practice.[28] This is the most important transfer-law lesson for India: contractual promises are insufficient where foreign surveillance law or lack of remedies prevents effective protection.

The EU-US Data Privacy Framework adequacy decision of 2023 illustrates the continuing attempt to reconcile trade and rights. The Commission concluded that the United States ensures an adequate level of protection for personal data transferred to certified organisations under the framework, based on commitments including limitations and safeguards regarding U.S. intelligence access and a redress mechanism.[29] Whether the framework will withstand future legal challenge is beyond the scope of this paper, but its existence demonstrates that adequacy

[25] European Commission, Data Protection, available at: https://commission.europa.eu/law/law-topic/data-protection_en (last visited on 22 June 2026).
[26] Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries, OJ L 199/31, 7 June 2021.
[27] Case C-362/14, Maximillian Schrems v. Data Protection Commissioner, ECLI:EU:C:2015:650.
[28] Case C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd. and Maximillian Schrems, ECLI:EU:C:2020:559.
[29] Commission Implementing Decision (EU) 2023/1795 of 10 July 2023 pursuant to Regulation (EU) 2016/679 on the adequate level of protection of personal data under the EU-US Data Privacy Framework, OJ L 231/118, 20 September 2023.

is a dynamic and contestable legal process rather than a mere diplomatic label.

VI. Comparative Assessment: India and the EU

Issue	India: DPDP Act/Rules	European Union: GDPR
Default transfer position	Transfers generally permitted unless restricted by Central Government notification or order.	Transfers permitted only if Chapter V conditions are satisfied.
Core legal method	Negative-list and executive specification model.	Adequacy, appropriate safeguards and limited derogations.
Localization	No general localization; targeted localization possible for specified data/significant fiduciaries and sectoral laws.	No general localization; protection follows data through safeguards.
Institutional design	Transfer restriction power mainly with Central Government; Board has adjudicatory functions.	Commission, supervisory authorities, EDPB and CJEU share roles.
Business certainty	Flexible but criteria for restriction are underdeveloped.	Higher compliance burden but clearer transfer tools.
Foreign State access	Rule 15 specifically addresses making data available to foreign States or controlled entities.	Foreign public authority access central to adequacy and Schrems analysis.

The comparison reveals that both systems are concerned with the same problem but use different legal techniques. India's model is facilitative and executive-led. The EU's model is rights-based, institutional and procedurally dense. India avoids the immediate burden of requiring adequacy or contractual transfer mechanisms for every transfer. This may be commercially efficient, particularly for a developing digital economy with strong service exports. However, it also means that businesses do not yet have a codified set of transfer safeguards comparable to the GDPR. In high-risk transfers, they must infer good practice from general obligations and sectoral expectations rather than rely on a comprehensive transfer toolkit.

The EU model is more demanding but more predictable. A controller can identify the

transfer route: adequacy, SCCs, BCRs or derogation. The exporter must examine whether the mechanism works in the recipient country, especially after Schrems II. This produces compliance costs, but it also builds trust. The Indian model can achieve similar trust only if the Government clarifies how it will use the section 16 power and Rule 15 orders. A list of restricted jurisdictions without reasons would not be enough. A structured risk framework would be more credible.

There is also a difference in rights culture. The GDPR gives data subjects extensive rights and connects transfer rules to effective remedies. India gives data principals rights of access, correction, erasure, grievance redressal and nomination, but the transfer chapter itself does not create a right to be informed of the recipient country, transfer mechanism or safeguards. The GDPR requires information about intended transfers, adequacy and safeguards in notices. India could improve transparency by requiring data fiduciaries to disclose categories of recipient countries, transfer purposes and safeguards in a clear privacy notice.

However, the EU should not be treated as a perfect model for India. The GDPR's compliance burden is significant, and India's legal and economic context differs. A strict adequacy model may be administratively heavy and may slow Indian innovation. India also has unique digital public infrastructure and financial inclusion priorities. The better lesson from the EU is not mechanical transplantation but institutional discipline: clear criteria, risk assessment, enforceable safeguards, independent supervision and judicially reviewable decisions.[30]

VII. Digital Trade and the GATS Framework

International trade law enters the debate because data restrictions affect trade in services. The General Agreement on Trade in Services applies to measures by WTO Members affecting trade in services.[31] Digital services frequently depend on cross-border supply. A cloud service, online legal database, financial analytics product, remote medical consultation, digital education service or software platform may be supplied from one territory into another without the supplier physically entering the consumer's country. If the service cannot lawfully receive, process or transmit data across borders, the ability to supply the service may be materially

[30] Regulation (EU) 2016/679, arts. 44-49; Commission Implementing Decision (EU) 2021/914, OJ L 199/31, 7 June 2021.
[31] General Agreement on Trade in Services, 1994, art. I.

impaired.

GATS obligations are structured around general obligations and scheduled commitments. Market access under Article XVI and national treatment under Article XVII apply where a Member has undertaken relevant commitments in its schedule.[32] A localization requirement could, depending on the sector and commitment, operate as a limitation on cross-border supply or a condition that disadvantages foreign suppliers. Even where it does not formally discriminate, it may increase costs by requiring local infrastructure, duplicated storage, local compliance teams and altered data architecture.

The most important protection for privacy regulation is Article XIV(c)(ii). It permits measures necessary to secure compliance with laws or regulations relating to the protection of the privacy of individuals in relation to processing and dissemination of personal data and the protection of confidentiality of individual records and accounts.[33] This provision is critical because it shows that WTO law recognises privacy as a legitimate regulatory objective. Privacy is not automatically subordinate to trade. However, the chapeau of Article XIV requires that such measures not be applied in a manner that constitutes arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services.[34]

The legal test therefore asks more than whether the State invokes privacy. The measure must be genuinely connected to privacy law or confidentiality, necessary in relation to that objective and administered in a non-arbitrary manner. For India, this means that transfer restrictions under section 16 should not be based on opaque political preference. If India restricts transfer to a jurisdiction, it should be able to show objective risk factors: absence of privacy law, excessive government access, weak enforcement, lack of remedies, cybersecurity concerns or inability to ensure onward transfer protection. Conversely, if a localization rule is introduced for a sector, India should assess whether less trade-restrictive safeguards would achieve the same purpose.

The WTO's own explanation of the GATS identifies four modes of supply and confirms

[32] Id., arts. XVI and XVII.
[33] Id., art. XIV(c)(ii).
[34] Id., art. XIV chapeau.

that cross-border supply is a recognised mode of international services trade.[35] This matters because many data-dependent services are supplied through Mode 1. A rule requiring all data to be processed locally may push foreign suppliers toward commercial presence, altering the economics of market access. Localization can therefore function like a market-entry condition.

The WTO e-commerce context further demonstrates the increasing importance of data governance. At the 13th Ministerial Conference in 2024, Members agreed to maintain the practice of not imposing customs duties on electronic transmissions until MC14 or 31 March 2026, whichever was earlier. The WTO's post-MC14 briefing note records that Members were unable to reach consensus on e-commerce at MC14 and that the Work Programme and moratorium lapsed on 30 March 2026.[36] This development shows that digital trade governance remains contested. Developing countries, including India, have strong reasons to preserve regulatory space, but they also benefit from stable and trusted digital trade rules.

A balanced trade-law position would reject both extremes. On one side, trade agreements should not prohibit legitimate privacy regulation. On the other side, privacy should not become a blanket justification for data protectionism. The best approach is interoperability: domestic privacy laws should require safeguards and accountability while allowing data to flow where adequate protection exists. This approach is compatible with GATS Article XIV because it treats privacy as a real objective and uses proportionate means.[37]

VIII. Data Localization: Does It Protect Privacy?

Data localization is often defended as necessary for privacy, but territorial storage alone does not guarantee privacy. Data kept in India can still be misused if access controls, encryption, audit logs, retention limits and remedies are weak. Data stored abroad can be protected if it is encrypted, subject to strong contractual and regulatory safeguards, and accessible only under lawful and proportionate conditions. Privacy is therefore a function of governance, not merely geography.

[35] WTO, Services: The GATS — Objectives, Coverage and Disciplines, available at: https://www.wto.org/english/tratop_e/serv_e/GATSqa_e.htm (last visited on 22 June 2026).
[36] WTO, E-commerce: Post-MC14 Briefing Note, available at: https://www.wto.org/english/thewto_e/minist_e/mc14_e/briefing_notes_e/ecommerce_e.htm (last visited on 22 June 2026).
[37] General Agreement on Trade in Services, 1994, art. XIV(c)(ii).

Localization may nevertheless serve legitimate purposes in some settings. Payment systems, critical infrastructure, defence, public health emergencies and regulatory supervision may require timely access to data by domestic authorities. The RBI payment data regime is an example of a sectoral supervisory model. Rule 13(4) of the DPDP Rules also contemplates that specified personal data and traffic data of Significant Data Fiduciaries may be kept from being transferred outside India where the Government so specifies.[38] Such targeted localization may be defensible where the category of data is clearly identified, the risk is high and the purpose cannot be achieved through less restrictive safeguards.

The danger lies in blanket localization. Scholarship on data nationalism warns that localization can fragment the internet, increase costs, reduce access to global services and empower State control without necessarily improving privacy.[39] Studies and policy papers on data restrictions similarly show that localization measures differ widely in intensity and may affect digital services trade.[40] OECD work has also mapped the growth and variety of localization measures and their potential implications for business activity.[41] The legal lesson is that localization should be exceptional, targeted and justified by evidence.

India's current statutory posture is relatively balanced because the DPDP Act does not impose general localization. However, the combination of section 16, Rule 13(4), Rule 15 and sectoral rules could become burdensome if used without coordination. A company may face a general transfer rule under DPDP, a sectoral storage rule from a financial regulator and special orders regarding foreign State access. Without harmonisation, compliance could become fragmented. This would harm both privacy and trade because confusion weakens implementation.

IX. India-EU Data Relations and the Adequacy Question

For Indian businesses, the EU is not merely a comparison point; it is a trading partner and a regulatory gateway. Indian IT and outsourcing firms often process data of EU customers. Where personal data of EU data subjects is transferred to India, the transfer must comply with

[38] The Digital Personal Data Protection Rules, 2025, rr. 13(4) and 15.
[39] Anupam Chander and Uyen P. Le, 'Data Nationalism', 64 Emory Law Journal 677 (2015).
[40] Martina F. Ferracane, Restrictions on Cross-Border Data Flows: A Taxonomy, ECIPE Working Paper No. 1/2017, available at: https://ecipe.org/publications/restrictions-to-cross-border-data-flows-a-taxonomy/ (last visited on 22 June 2026).
[41] Chiara Del Giovane, Janos Ferencz and Javier López-González, The Nature, Evolution and Potential Implications of Data Localisation Measures, OECD Trade Policy Paper No. 278 (2023).

GDPR Chapter V. India does not presently have an EU adequacy decision. Therefore, EU-to-India transfers generally require appropriate safeguards such as standard contractual clauses, and after Schrems II exporters must assess whether Indian law and practice allow the clauses to operate effectively.[42]

An EU adequacy decision for India would be commercially valuable, but it would require more than enactment of the DPDP Act. The Commission's adequacy analysis examines rule of law, respect for human rights, relevant legislation, data protection rules, security, public authority access, independent supervisory authorities and effective administrative and judicial redress.[43] India's recognition of privacy as a fundamental right is a strong foundation. The DPDP Act's creation of rights and obligations is also relevant. However, broad government exemptions, executive control over transfers and questions regarding independence and resources of the Data Protection Board may require careful attention.

India should not design its privacy law solely to satisfy the EU. That would be neither democratically necessary nor developmentally appropriate. Nevertheless, EU adequacy criteria provide useful benchmarks for trusted data governance. If India strengthens transparency around government access, creates clearer safeguards for international transfers, improves Board independence and provides effective remedies, it would improve domestic constitutional protection as well as international data-flow credibility. Adequacy should therefore be viewed not as external pressure but as an opportunity to align rights and trade.

X. Recommendations

First, India should publish objective criteria for using the section 16 power. These criteria should include the recipient country's privacy law, independent supervision, remedies, limits on government access, cybersecurity environment, onward transfer rules and international cooperation. The criteria need not copy the GDPR, but they should be transparent enough to prevent arbitrary restriction.[44]

[42] Regulation (EU) 2016/679, arts. 44, 45 and 46; Case C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd. and Maximillian Schrems, ECLI:EU:C:2020:559.
[43] European Commission, Data Protection Adequacy for Non-EU Countries, available at: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (last visited on 22 June 2026).
[44] The Digital Personal Data Protection Rules, 2025, r. 15; Regulation (EU) 2016/679, art. 45(2).

Secondly, India should introduce standard contractual clauses or model transfer clauses under the DPDP framework. Such clauses would provide commercial certainty to Indian businesses and improve protection for data principals. They should include purpose limitation, security safeguards, sub-processing controls, breach notification, assistance with data principal rights, onward transfer restrictions and remedies. A clause-based model would be less burdensome than mandatory adequacy for every transfer but more protective than silence.

Thirdly, India should require transfer impact assessment for high-risk transfers. The trigger may be large-scale processing, children's data, financial data, sensitive contexts, transfer to jurisdictions with weak safeguards or involvement of foreign public authority access. The assessment should examine whether the legal and technical safeguards are effective in practice. This would translate the Schrems II lesson into an Indian risk-based model without mechanically importing EU law.

Fourthly, data principals should receive clearer notice regarding international transfers. Privacy notices should disclose categories of recipient countries, transfer purposes, classes of recipients and safeguards. This is important because consent or lawful processing becomes meaningful only when individuals understand material transfer risks.

Fifthly, India should harmonise sectoral localization rules with the DPDP Act. Financial, health, telecom and critical infrastructure regulators may need stricter rules, but those rules should be mapped against DPDP obligations. A common governmental guidance document could reduce conflicts and compliance duplication.

Sixthly, the Data Protection Board should have a meaningful role in transfer governance. While foreign affairs and national security may justify executive involvement, data protection requires independent oversight. The Board could issue guidance, review compliance with transfer safeguards and publish anonymised decisions.

Seventhly, India's WTO and digital trade policy should preserve privacy regulatory space while avoiding unnecessary restrictions. India can defend genuine privacy measures under GATS Article XIV, but it should design them to satisfy necessity and non-discrimination. This will help India resist pressure for unrestricted data flows while avoiding claims of disguised

protectionism.[45]

XI. Conclusion

Cross-border data transfer law is the legal infrastructure of the digital economy. India's DPDP Act and Rules represent a major step toward comprehensive privacy governance, but the transfer framework remains in an early stage of institutional development. The Indian model is commercially flexible because it avoids general localization and allows transfers unless restricted. That flexibility is valuable for India's technology sector and service-export economy. However, flexibility must be matched with transparency, safeguards and remedies. Without these, the system may appear unpredictable to businesses and insufficiently protective to individuals.

The EU's GDPR demonstrates a different model. It does not localize all data within Europe, but it insists that protection travel with the data. Adequacy decisions, standard contractual clauses, binding corporate rules and derogations form a structured transfer architecture. The Schrems litigation shows that foreign surveillance and lack of effective remedies are not peripheral issues; they are central to the legality of cross-border transfers. India can learn from this without copying the GDPR wholesale.

International trade law confirms that privacy and trade are not mutually exclusive. GATS Article XIV expressly recognises privacy protection in relation to personal data, but it also disciplines arbitrary and disguised restrictions. Data localization may be justified in targeted sectors, but blanket localization is rarely the most privacy-protective or trade-compatible tool. The future lies in trusted data flows: transfers supported by enforceable safeguards, accountable institutions and proportionate regulation.

India should therefore develop a transparent, risk-based and rights-oriented transfer regime. It should publish restriction criteria, create model clauses, require high-risk transfer assessments, strengthen independent oversight and harmonise sectoral localization. Such reforms would protect Indian data principals, support Indian businesses, improve prospects for India-EU data cooperation and position India as a credible rule-maker in global digital trade governance.

[45] General Agreement on Trade in Services, 1994, art. XIV(c)(ii); WTO, E-commerce: Post-MC14 Briefing Note, supra note 35.