DATA SOVEREIGNTY AS AN ENTERPRISE RISK: LOCALISATION STRATEGY, REGULATOR-TO-REGULATOR CO-OPERATION UNDER INDIA'S DIGITAL PERSONAL DATA PROTECTION ACT, 2023

Maitry Kumari, BSc LLB (Hons.), National Forensic Sciences University, Gandhinagar

Tanbi Bhadani, BBA LLB (Hons), Chanakya National Law University, Patna

ABSTRACT

Data sovereignty has emerged as an increasingly important enterprise risk in contemporary regulatory discourse, warranting strategic governance at the board and C-suite levels. India's Data Protection Act, functionally operationalised through rules notified in November 2025, emerged as a calibrated, risk-proportionate framework for personal data governance, embodying the SARAL (Simple, Accessible, Rational, Actionable and Lawful) design principles. Unlike rigid data localisation regimes, the statute vests the State with discretionary authority to restrict cross-border personal data flows on a permissioned, case-by-case basis, thereby maintaining the balance between national data sovereignty imperatives and international data transfer obligations under the law of trade and investment.

This article interrogates the amalgamation of data sovereignty and enterprise risk management (ERM), placing the DPDP act in the context of the global data protection regulatory ecosystem and a growing body of adequacy decision jurisprudence. Using doctrinal and comparative regulatory scholarship, the paper identifies the transactional and operational risks associated with data sovereignty regulations, particularly those related to the M&A process, third-party vendor management, digital transformation of the global supply chain, and multi-cloud and hybrid cloud procurement. In this respect, the study indicates that the cost of compliance due to data residency and localisation requirements amounts to 15-30% of operational technology costs in MNEs. In this case, it is important to consider a strategy for responding to these challenges. Therefore, the paper discusses the viability of layered data residency architectures and privacy-enhancing. technologies (PETs) such as pseudonymization, end-to-end encryption, tokenisation, and differential privacy as tools of regulatory compliance while maintaining operational interoperability.

Keywords: Data Sovereignty, Digital Personal Data Protection Act 2023, cross-border data flow, enterprise risk, Data localisation, adequacy decision.

I. Introduction

In a contemporary regulatory discourse, data sovereignty has metamorphosed into to a fundamental enterprise risk from peripheral compliance concern that seeks board level attention. The Digital Personal Data Protection (DPDP) Rules 2025, notified in November, have finally operationalised the "SARAL" (Simple, Accessible, Rational, Actionable) framework envisioned in 2023[1]. For the modern enterprise, data is no longer just an asset; it is a high-stakes liability. Unlike its abandoned predecessor, the Personal Data Protection Bill, 2019 contained a prescriptive data localisation requirement and the current act adopts a more calibrated approach[2]. Section 16 empowers the state to restrict cross border data transfer to the negative list countries, instead of imposing blanket localisation mandates.

This regulatory architect ought to be understood within the broader global context. The EU's GDPR pioneered comprehensive Privacy regulation with its adequacy framework for international transfers[3]. The US has adopted a sectoral approach having laws for state levels that are comprehensive like in California (CPPA)[4], Virginia (VCDPA)[5], and Colorado (CPA)[6] while lacking federal omnibus legislation. China's Personal information Protection Law (PIPL) and Cybersecurity Law Mandate extensive localisation for critical information infrastructure operators and large-scale processors[7]. Enterprises that operate in multiple jurisdictions so to work smoothly these divergent regulatory approaches created an intricate compliance matrix. Data Sovereignty has become a strategic risk factor affecting the market entry decisions, M&A valuations, supply chain architecture since it is not just limited to legal or It deliberations This article examines data sovereignty through the lens of enterprise risk management, analyzing localisation strategies and the emerging framework for regulator- to-regulator cooperation, with particular focus on how business should respond to India's DPDP Act and its

[1] Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), Gazette of India, Extraordinary, Part II, § 3(i) (Nov. 13, 2025).
[2] The Personal Data Protection Bill, 2019, Bill No. 373 of 2019, Lok Sabha (India), introduced Dec. 11, 2019.
[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 Apr. 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), 2016 O.J. (L 119) 1, available at https://gdpr-info.eu/
[4] California Privacy Protection Agency, https://cppa.ca.gov/ (last visited June 5, 2026).
[5] Va. Code Ann. §§ 59.1-575 to -585 (2025).
[6] Colorado Privacy Act (CPA), Consumer Privacy Act, https://www.consumerprivacyact.com/colorado-privacy-actcpa/ (last visited June 19, 2026).
[7] Personal Information Protection Law, https://personalinformationprotectionlaw.com/ (last visited June 19, 2026).

implementing rules notified on November 2025.

II. Foundation of Data Sovereignty

The evolution of the data economy has progressed through three distinct eras: Centralisation (the 2000s), Cloudification (the 2010s), and now Sovereignization (the 2020s). In 2026, the underlying tension lies between the data ownership and data control. For Indian business specifically those operating cross borders, the act reframes personal data as a regulated economic asset subject to sovereign oversight rather than a freely transferable commodity. Ownership of customer data may belong to the corporation, but the sovereignty is shifting towards the state. The Digital Data Protection Act transformed data from a global flow into a national asset. The concept establishes a psychological and legal connection between the person and their data, which remains protected by the Indian state. Therefore, it does not mandate absolute localisation rather it established as a conditional mobility where the data can move across borders unless restricted by the government notification (section 16(1)). This creates a dynamic risk landscape where regulatory posture can be amended based on geopolitical, economic or security considerations.

III. The legal and Regulatory Landscape

Data localisation requirements significantly raise both direct and indirect costs for enterprises. Results of a Deloitte 2024 survey of 500 multinational companies in the Asia-Pacific region found that more than two-thirds (73%) indicated their firm was spending an additional 15-30% on operations to comply with varying data localisation demands led most notably by financial services and healthcare[8]. The DPDP Rules, 2025[9] impose various granular obligations on Data Fiduciaries such as the requirement to adopt security safeguards for data protection (Rule 6)[10], notification of a personal data breach (Rule 7),[11] and time-based retention and disposal of

[8] Bill Briggs & Mike Bechtel, *Tech Trends 2024: Generative AI—Force Multiplier for Human Ambitions* (Deloitte Insights 2024), available at https://www.deloitte.com/content/dam/insights/articles/2024/us176403_tech-trends2024/di-tech-trends-2024.pdf

[9] Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), Gazette of India, Extraordinary, Part II, § 3(i) (Nov. 13, 2025), available at https://www.meity.gov.in/static/uploads/2025/11/53450e6e5dc0bfa85ebd78686cadad39.pdf

[10] Digital Personal Data Protection Rules, 2025, r. 6, G.S.R. 846(E), Gazette of India, Extraordinary, Part II, § 3(i) (Nov. 13, 2025).

[11] Digital Personal Data Protection Rules, 2025, r. 7, G.S.R. 846(E), Gazette of India, Extraordinary, Part II, § 3(i) (Nov. 13, 2025).

personal data (Rule 8)[12].

The MNCs had a centralized global system where compliance attracts hefty investments in infrastructure. The cloud service models based on redundancy and geographical distribution for better performance need to be reoriented to fit in jurisdictional limits. The requirement under Rule 6(1)(a) for "appropriate data security measures, such as securing personal data through encryption, obfuscation, masking, or the use of virtual tokens" applies regardless of where the data is located[13]. However, implementing these measures becomes much more complicated when data must be separated by jurisdiction. The Information Technology and Innovation Foundation (ITIF) in its study found that forced data localization measures cut GDP by 0.7 to 1.7% in countries that adopt such policies, leading to global welfare losses estimated at $63 billion every year[14]. Take, for example, a multinational e-commerce platform that operates across APAC markets[15]. Under the DPDP framework, if the Central Government limits data transfers to certain countries under Section 16, the e-commerce platform needs to have a separate data processing landscape each with its own encryption key management, access controls, audit logs, and backup systems. The Third Schedule of the Rules sets specific data retention periods for different types of Data Fiduciaries, such as three years for e-commerce entities with at least 20 million registered users in India, therefore this requires jurisdiction specific data lifecycle management. Thus, the compliance burden extends beyond the jurisdiction[16].

IV. **Strategic Operational Challenges Across Business Functions**

Data sovereignty requirements impose structural challenges to not just one but several operational dimensions and change at the core how global enterprises design their business

[12] Digital Personal Data Protection Rules, 2025, r. 8, G.S.R. 846(E), Gazette of India, Extraordinary, Part II, § 3(i) (Nov. 13, 2025).

[13] *Digital Personal Data Protection Rules, 2025*, r. 6, G.S.R. 846(E), Gazette of India, Extraordinary, Part II, § 3(i) (Nov. 13, 2025).

[14] Nigel Cory & Luke Dascoli, *How Barriers to Cross-Border Data Flows Are Spreading Globally: What They Cost and How to Address Them* (Information Technology & Innovation Foundation, July 2021), available at https://www.researchgate.net/publication/353368028_How_Barriers_to_Cross-Border_Data_Flows_Are_Spreading_Globally_What_They_Cost_and_How_to_Address_Them.

[15] What Is APAC Region Countries?, StudyCountry, https://www.studycountry.com/wiki/what-is-apac-regioncountries (last visited June 6, 2026).

[16] Digital Personal Data Protection Rules, 2025, sch. III, G.S.R. 846(E), Gazette of India, Extraordinary, Part II, § 3(i) (Nov. 13, 2025).

processes.

A. Cross-Border M&A and Corporate Restructuring: One of the requirements of a proper M&A due diligence nowadays is to appraise the level of data sovereignty compliance as one of the material risks in the transaction. According to EY's 2024 Global Corporate Divestment Study, 42% of crossborder technology acquisitions had to be adjusted more than 10% in valuation due to data localization compliance gaps identified through due diligence, which in turn led to these postclosing adjustments[17]. With increasing frequency, share purchase agreements include in their representations and warranties special clauses on data storage locations, mechanisms for crossborder data transfers and the regulatory compliance status.

B. Section 17(1)(e) of the Act is an exemption for processing necessary for a scheme of compromise or arrangement or merger or amalgamation is a very limited concession as it only exempts such processing from Chapters II and III and does not grant immunity from all other requirements[18]. Therefore, acquiring companies will need to perform extensive data mapping exercises to find, analyse, and quantify data stored in the respective locations as well as calculate the costs of the restructuring that will give rise to compliance with the data protection laws post-transaction.

C. Global Supply Chain Integration: A modern supply chain usually is characterized by data flows amongst manufacturers, logistics, and distributors crossing borders. According to a 2023 McKinsey report, supply chain disruptions have data governance issues in 68% of cases as opposed to only 23% in 2019[19]. Rule 15 states that the cross-border transfer of any personal data processed under the DPDP Act shall be subject to the compliance with the requirements set by the Central Government, "in respect of making such personal data available to any foreign State, or to any person or entity or any agency under the control of such State"[20]. This makes it difficult for globally integrated companies to know if and when they can cross the

[17] EY's 2024 Global Corporate Divestment Study
[18] Digital Personal Data Protection Act, No. 22 of 2023, § 17 (India).
[19] Michael Chui, Roger Roberts, Lareina Yee, Alex Singla & Alexander Sukharevsky, *The State of AI in 2023: Generative AI's Breakout Year*, McKinsey & Co. (Aug. 1, 2023), https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-in-2023-generative-ais-breakoutyear
[20] Digital Personal Data Protection Rules, 2025, r. 15, G.S.R. 846(E), Gazette of India, Extraordinary, Part II, § 3(i) (Nov. 13, 2025).

border with their data because as they must wait for the specific orders allowing transfer mechanisms.

D. Cloud Service Procurement: The model of a hyperscale cloud mostly relies on dynamically reallocating resources among different global regions. Enterprises pursuing compliance with DPDP (Data Protection and Digital Privacy) must impose contractual terms with cloud service providers (acting as Data Processors) that will guarantee data residency and sovereignty requirements. Rule 6(1)(f) requires the "contract between the Data Fiduciary and the Data Processor" to have "appropriate provision" relating to security safeguards[21]. Yet, as Gartner pointed out in its 2024 Cloud Services Market Analysis[22], Standard cloud service contracts usually are averse to making commitments on data residency from the client's perspective due to architectural complexity and cost implications. Hence, it creates negotiating friction and could facilitate rich pricing tiers for guaranteed in-country processing.

E. Competitive and Strategic Risks

In addition to the operational issues that arise, data sovereignty rules bring about strategic risks that can even change the current competitive landscape:

Market Access Barriers: In fact, if strong localisation requirements are used as a non-tariff barrier to trade, then a smaller or new foreign company who doesn't have local infrastructure will be at a greater disadvantage. The domestic rivals who already have their local operations may potentially be the ones to benefit, which therefore leads to the suspicion that data sovereignty is just a fig leaf for protectionism.

A. **Innovation Constraints:** Developing advanced analytics, machine learning, and AI is highly dependent on having big and diversified datasets. Therefore, if we limit data flows to within national boundaries, these kinds of technologies may not be as effective. For example, a multinational health tech company will face challenges in creating diagnostic algorithms if they are not allowed to use the data of Indian patients together with other global datasets for training the model.

[21] Digital Personal Data Protection Rules, 2025, r. 6, G.S.R. 846(E), Gazette of India, Extraordinary, Part II, § 3(i) (Nov. 13, 2025).

[22] Chris Laske, Chris Saunderson & Chris Matchett, *Let the Robots Enhance Your ITSM Service Desk* (Gartner, Inc. Dec. 21, 2023), https://www.gartner.com/en/documents/5078231

B. **Technology Lock-In:** Making data architectures for different jurisdictions might lead to a situation of vendor lock-in since it will be harder to switch cloud providers once the data has to be kept in certain geographical locations. Hence, the negotiating power is diminished and the overall cost of ownership increases.

C. **Regulatory Arbitrage Risks:** The data sovereignty rules of different jurisdictions are not fully aligned and as a result businesses are given an opportunity for regulatory arbitrage. They can, for example, organize their structure such that the Indian operation would be too small to be designated as a Significant Data Fiduciary, and thus avoid the obligations that come with the designation. Of course, from a pure risk perspective, such an approach may be justified but it may not be in line with the overall business goals.

V. Global Localisation Precedents and Comparative Analysis

India's implementation of data localisation under the DPDP Act needs a comparison to:

A. The European Union's GDPR and Post-Schrems II Framework: GDPR represents the most impactful global privacy landscape extending beyond EU borders through the 'Brussels Effect[23]'.

The approach towards the cross-border data transfer is fundamentally different from localisation mandates and it allows transfer of data to the countries having "adequate" data protection laws or via Standard Contractual Clauses or Binding Corporate Rules. The European Commission has granted adequacy decisions to 14 jurisdictions including the UK, Japan, South Korea, Canada (for commercial organizations) as of 2024[24]. These decisions basically determine the free flow of data without any additional safeguards which create significant data corridors. However, the CJEU[25] invalidated the former framework and struck down the EU-US Privacy Shield requiring data exporters to conduct case by case assessments of the privacy framework in the destination countries and implement supplementary measures to ensure the equivalence of GDPR and incorporated mandatory transfer impact assessments. Moreover, EDPB issued detailed recommendations for the security and organisational measures limiting the government access.

[23] Anu Bradford, The Brussels Effect: How the European Union Rules the World 3-28 (2020).
[24] European Commission, Adequacy Decisions (updated Jan. 2024)
[25] Court of Justice of the European Union.

B. China's Comprehensive Localisation Model: The PIPL, China's personal data protection law, which came into effect in November 2021, and the Cybersecurity Law, both set the bar extremely high for data localisation in the world. CIIOs must keep the personal information and important data they have collected within China inside the country. In case of cross-border transfer, a security assessment has to be conducted by the Cyberspace Administration of China (CAC) or the parties have to use standard contractual clauses approved by CAC. This ensures almost complete data isolation for sensitive sectors.

C. ASEAN Framework on Digital Governance: The association of southeast Asian Nations adopted a framework in 2024 encouraging interoperability data protection framework while considering domestic sovereignty which includes Mutual Recognition of privacy Certifications, Cooperation in Cross-border enforcement, Development of regional adequacy assessments and capacity building for authorities of data protection. Now the participation of India in such a regional initiative could facilitate data transfer with ASEAN economies Significant trade partners for India's digital economy.

D. India's DPDP legislation, which grants the government the power, under Section 16, to restrict cross-border data transfers on a case-by-case basis instead of a blanket data localisation requirement, is somewhat between the permissive EU framework and the restrictive China-Russia model. However, while it gives more room for manoeuvre, it also leads to a lack of certainty as companies will only be able to find out which cross-border data transfers have been prohibited once the government issues specific notifications**.** The EU commission and Indian Ministry of Electronics and IT have engaged in preliminary adequacy decisions, yet there exist gaps. The EU's adequacy decisions comprise of rule of law and dignity for human rights, the existence of an impactful data protection framework, existence of independent supervisory authorities and international commitments. So, if India includes these robust principles EU adequacy recognition could create a substantial data corridor with advantageous to Indian service exporters and European companies with Indian Operations. Similarly, India can participate in such bilateral negotiations with the traders and set up an independent review mechanism for the government's access to data, and introduce certification programs for the organizations backed by the law.

VI. Enterprise Localisation Strategies

Smart corporations tend to pursue hybrid approaches that give them some leeway for

compliance while they keep up their business productivity**:**

A. Tiered Data Residency Architecture

Organizations mostly apply multi-tier data classification frameworks that match the localisation requirements to the level of data sensitivity.

- **Sovereign Data (Tier 1):** The personal data of Indians (data principal) as per DPDP, which is processed, stored within the Indian Jurisdiction and with no cross- border transfers and is collected for the India specific services.

- **Controlled Cross-Border data (Tier 2):** Transfer of personal data with legitimate business purposes like global customer support, transferred only via complying Rule 15.

- **Global data (Tier 3):** The anonymized, aggregated or non personal data falls outside the scope of DPPD and is processed in an optimized infrastructure irrespective of the geographical restriction.

With this approach, companies are required to have data classification at a very granular level and to implement strong technical measures that will prevent any unauthorized data flow from one tier to another.

B. Regional Data Centre Deployments

Leading cloud providers and large corporations are creating regions dedicated to India**:**

- Microsoft Azure**:** Runs three data center regions in India (Central India, South India, West India), allowing customers to keep their data in India.

- Amazon Web Services**:** For local data processing, AWS enables the Asia Pacific (Mumbai) region with multiple availability zones.

- Google Cloud**:** Locations of Google Cloud services in Mumbai and Delhi are geared toward Indian data residency requirements.

By employing these platforms, organizations can put geographical restrictions in place so that Indian personal data stays within the Indian borders, and yet take advantage of global

infrastructure for other types of work. Nonetheless, this method shall be configured in a very meticulous manner - simply picking an Indian region will no longer be enough if backup, disaster recovery, or operations data sharing lead to transferring data abroad.

C. Contractual Data Processing Frameworks

The Rule 8 instructs Data Fiduciaries to have valid contracts in place when they engage Data Processors, and Rule 6(1)(f) goes further in requiring "appropriate provision in the contract" for security safeguards. The most comprehensive Data Processing Agreements (DPAs) from the practice point of view should contain:

- **Scope Limitation:** Unambiguously specify what kinds of personal data will be processed and what processing purposes are allowed, in accordance with the Data Fiduciary's notices to Data Principals.

- **Data Residency Commitments:** Clear statements about the physical location of data storage and processing, and the agreement that any violation will be classified as a major default.

- **Sub-Processor Controls:** Provisions that the Data Processor needs to obtain the Data Fiduciary's approval before signing a contract with any sub-processor, and that they must pass on the same level of responsibilities.

- **Audit Rights:** The Data Fiduciary shall have the right to perform audits of the Data Processor’s DPDP compliance, which may include inspection (either on-site or remote) of data storage facilities/premises.

- **Data Breach Protocols:** The agreement shall specify the time limits within which the Data Processor must notify the Data Fiduciary of any personal data breach the moment the Data Processor becomes aware of this, thus the Data Fiduciary will be able to satisfy the 72hour notification requirement to the Data Protection Board under Rule 7.

- **Data Erasure and Retention:** Procedures for deleting and retaining the data once the purpose has been served or withdrawal of consent or any reason as per the DPDP by the Data fiduciaries.

D. Technical Safeguards: Encryption and Tokenization

Rule 6(1)(a) includes encryption, obfuscation, masking or the use of virtual tokens mapped to the personal data in the list of security measures that can be used. Developing entities are adopting:

- **Format-Preserving Encryption:** The data is encrypted and yet the format is preserved for the operational use, thus the decryption keys in this case are held only in India.
- **Tokenization for Cross-Border Transfers:** The sensitive personal data is substituted with non-sensitive tokens for international processing, with only the mapping table kept in India. Therefore, the whole world can be engaged (e.g., a fraud detection system will be able to analyse the pattern of transactions) with no transfer of actual personal data abroad.
- **Homomorphic Encryption:** This new encryption technique allows processing encrypted data and sending the result when data is decrypted without accessing the data itself. This kind of cryptographic method thus made it possible to perform operations on encrypted data that were previously unimaginable. Cross-border processing while still preserving data sovereignty may become possible with this method.

VII. Regulator to Regulator Cooperation: Cross- Border Data Transfer

On the point of how regulators need to collaborate, it's mainly because data moves around and doesn't stay in one location. Just think of a typical online purchase; the customer's information might be processed in India, the payment might be handled in Singapore, the US might conduct the fraud checks, and the logistics could be managed in Dubai. Confining businesses only to the national laws thus makes the cross-border transactions very challenging, in fact, almost not possible for the legit things. Regulatory cooperation could be the way forward, as it reconciles the notions of sovereignty with real-world requirements.

A. **Mutual recognition** is when countries agree that each other's privacy frameworks are good enough and data can flow without additional steps. The GDPR's adequacy decisions are a good example, the EU has approved 14 countries including Japan, South Korea, the UK under Article 45.

B. **Safe Harbor Agreement** are essentially negotiated deals with certain conditions for transfers.

The EU-US Data Privacy Framework from July 2023, after the old Privacy Shield was struck down by Schrems II, allows US companies to certify voluntarily for EU data, with commitments and mechanisms for resolving disputes.

C. **Standard contractual clauses (SCC)** are something else altogether, these are the templates that regulators approve for exporters and importers to use. The EU's updated SCCs from June 2021 require the parties to be bound by the transfer protection obligations.

D. **Conducting joint investigations** of data breaches of multinational companies or systematic non-compliance issues. For example, a unified investigation by India's Data Protection Board and European Data Protection Board of a breach on a global social media platform affecting Indian and EU users would be more productive than two separate investigations.

E. **Secondment Programs:** A temporary work exchange program where staff of the Indian Data Protection Board work in leading privacy authorities to enhance their regulatory skills.

F. **Technical Standard Harmonization**: Participate in international standard setting agencies for information security like in ISO or for privacy engineering standard like in IEEE. This will make sure that the leading privacy standards will recognize Indian needs.

G. **Sector-Specific Cooperation Protocols**: There are some sectors where the international cooperation should be carefully designed:

- **Financial Services**: Work with financial regulators (RBI, SEBI) to prepare mechanisms for cross-border data transfers which take into account the global financial system's requirements. The Bank for International Settlements and the International Organization of Securities Commissions invite platform for such coordination.

- **Healthcare and Life Sciences**: Data transfer is significant for genomic research or clinical trials so India might agree with the medical research authorities in specifies countries on research specific data transfer mechanism to allow scientific collaboration while protecting the data of Indian citizen.

- **Cloud and Digital Services**: participate in discussions with home regulators of major cloud service providers to establish cooperative oversight frameworks that will enable these global platforms to satisfy Indian requirements.

H. **Binding Corporate rules**: Apparently, the DPDP does not recognize the BCRs- the internal data protection policies are binding on entities within a corporate group which are approved by regulators. The data protection Board could develop BCR approval procedures which can permit multinational groups to transfer personal data among Indian and foreign affiliates as on the Bord's approved internal governance. BCRs would require comprehensive meeting DPDP standards moreover it requires enforceable rights for data principals- citizen of India against foreign group entities and Data protection Board audit authority over foreign compliance as well as IDR (Independent dispute resolution) mechanisms.

VIII. India's Emerging Cooperation Framework

Although the DPDP Act does not directly mention a collaboration with foreign regulatory bodies, the overall structure gives a hint that such cooperation is possible:

A. **Section 16 Discretionary Power**: The power of the Central Government to limit the transfer of data "to such country or territory outside India" through a notification indicates the opposite as well transfers to countries that are not notified in this way are still allowed. This way, India can open a list of countries to which data transfers are regarded as safe, which can be made dependent on a reciprocal recognition or bilateral agreement.

B. **Rule 15 Implementation Flexibility**: Rule 15 sets forth that cross-border data transfers should satisfy the "requirements that the Central Government may, by general or special order, specify." The wording here allows for differentiated requirements—for example, imposing strict rules for some countries and giving easy access to trusted partners. Thus, India can elaborate in detail on the privacy laws of other countries like an adequacy assessment.

C. **Bilateral and Plurilateral Negotiations**: India has been in talks with the European Union on the latter's potential adequacy recognition. There are quite a few issues that need to be resolved especially since India's surveillance regime and the issue of government data access are at the core of the matter—but, should the talks be successful, they would pave the way for an EU-India data flow channel which would be a great advantage to the businesses operating in both regions.

IX. Conclusion

Data sovereignty, introduced via the DPDP Act and its Rules, is a significant shift in the attitude

of enterprises toward data handling. Localisation alone cannot do the job. However, from an economic standpoint, the blanket localisation is unsustainable and perhaps can do more harm than good. The costs that getting businesses to shoulder infrastructure duplication, loss of advantages of scale, and reduction in innovation should be weighed against the privacy and security gains that are realistically achievable. Therefore, it is not the whole personal data that deserves similar treatment; the intensely private data (like health and financial records as well as biometric data) might well justify strict localisation whereas the non-sensitive commercial data (like business contact information and transactional data) could be routed without barriers to trusted jurisdictions.

The road to the future of data sovereignty lies in regulatory cooperation like bilateral adequacy decisions, participation in regional cooperation initiative. The business adaption imperatives require risk management as well such as data mapping and deployment of hybrid data architecture and investments in privacy enhancing technologies. Thus, data sovereignty should be perceived as a responsivity to ensure protected data processing irrespective of it location and considering the fundamental rights of data principals while enabling the legitimate commercial and business purpose. The path requires active cooperation and recognizing that in digitally intertwined economies, privacy protection is a shared global challenge that demands collaborative solutions.