DISMANTLING THE GDPR HEGEMONY: INDIA'S DPDP ACT AND THE RISE OF LEAN DATA GOVERNANCE IN THE GLOBAL SOUTH

Abhishek Mishra
Dual Degree Master's LL.M.
Student, National Forensic Sciences University,
India and Tashkent State University of Law, Uzbekistan
https://doi.org/10.5281/zenodo.21187047

Abstract

For nearly a decade, the European Union's General Data Protection Regulation (GDPR) has been heralded as the undisputed universal gold standard for data protection, prompting an aggressive wave of legal transplantation across developing nations. This article challenges this Eurocentric hegemony by analysing India's Digital Personal Data Protection (DPDP) Act, 2023, alongside its finalized DPDP Rules (2026), as a revolutionary counter model.

India has rejected the GDPR's hyper bureaucratic, litigation heavy framework in favour of a Lean Data Governance architecture. While the GDPR relies on individual notice and consent compliance mechanisms that systematically fail in developing economies due to stark digital literacy and enforcement asymmetries thus the DPDP Act leans into technology-embedded law.

Using a Third World Approaches to International Law (TWAIL) framework, this article evaluates how India's model shifts the regulatory burden off vulnerable individuals and onto architectural fiduciaries.

Keywords: Digital Personal Data Protection (DPDP), European Union's General Data Protection Regulation (GDPR), Lean Data Governance architecture, Third World Approaches to International Law.

Introduction

The Brussels Effect and Its Structural Misfit in Developing Economies

For over a decade, the European Union's General Data Protection Regulation (GDPR) has operated as the unchallenged global blueprint for data privacy legislation. This phenomenon, famously conceptualized by Anu Bradford as the Brussels Effect[1], occurs through a mix of market mechanisms and regulatory emulation. Multinational corporations, seeking to avoid fragmented compliance costs, standardized their global data processing practices around the strict mandates of the GDPR. Concurrently, dozens of jurisdictions stretching from Latin America to Southeast Asia copied the text of the GDPR into their domestic statutes, chasing adequacy decisions[2] to ensure uninterrupted data flows with the European market.

However, importing a regulatory model designed for a post-industrial, service heavy Western economy into the Global South has exposed deep structural misfits. The GDPR[3] is built on a high friction, process heavy framework. It relies on complex bureaucratic

[1] **The Brussels Effect**: Attributed to Anu Bradford. This concept explains how the EU's regulatory standards become global defaults through market mechanisms

[2] **Article 45 (Adequacy Decisions) EU GDPR:** Allows transfers to countries the European Commission deems have an "adequate" level of protection

[3] Article 2 EU GDPR: Defines the regulation's applicability to the processing of personal data by automated means or manual processing that forms part of a filing system

mechanisms: extensive Data Protection Impact Assessments (DPIAs)[4], continuous data mapping, mandatory records of processing activities (RoPA), and the institutionalization of specialized Data Protection Officers (DPOs).

While these administrative burdens are manageable for well-capitalized European enterprises, they impose severe costs on the economic realities of developing nations:

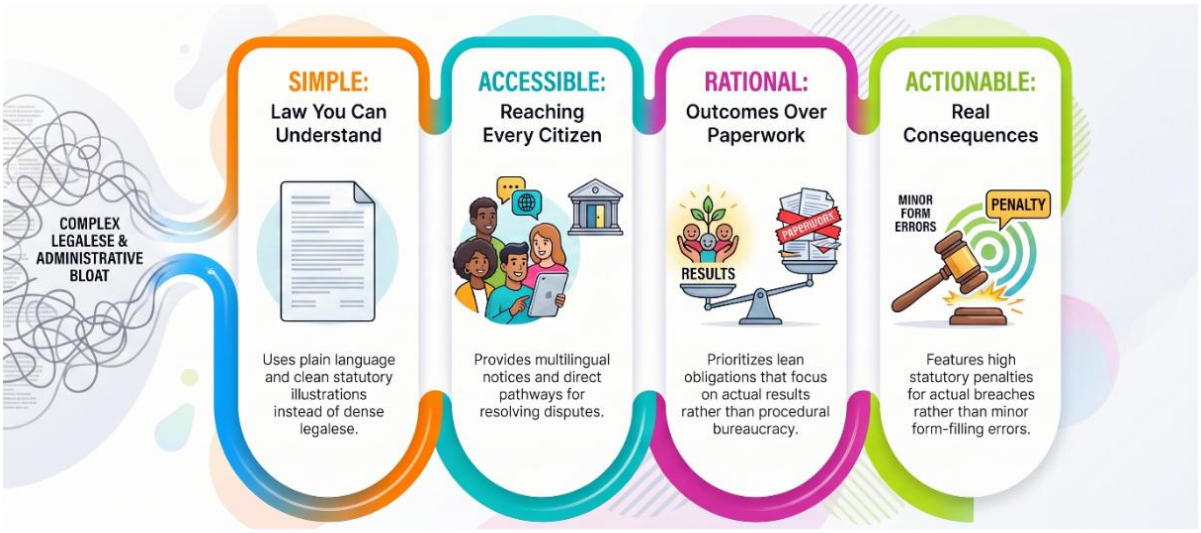
- **The MSME Bottleneck:** In developing economies, micro, small, and medium enterprises (MSMEs) form the backbone of GDP and employment. For an ordinary merchant or a growing software startup in a developing country, the compliance cost of a GDPR-style framework can be prohibitive, acting as a structural barrier to digitization.
- **The Literacy and Infrastructure Gap:** The GDPR assumes a high baseline of digital literacy among consumers, who are expected to navigate dense, multi-layered privacy policies. In contrast, emerging markets are often defined by rapid mobile internet adoption outpacing formal digital literacy.
- **The Enforcement Deficit:** Developing states frequently lack the fiscal resources and administrative capacity to fund and staff massive, hyper-bureaucratic data protection authorities capable of auditing millions of informal market actors.

Consequently, when the Global South blindly copies the GDPR, it often creates a system of paper compliance where laws exist on the books but are functionally unenforceable, stifling domestic innovation while failing to provide meaningful privacy protections to the public[5].

Material and Methods

Deciphering India's Lean Alternative: DPDP Act 2023

India's Digital Personal Data Protection (DPDP) Act, 2023, coupled with the finalized DPDP Rules notified by the Ministry of Electronics and Information Technology (MeitY) on November 13, 2025[6], represents a deliberate break from European regulatory inflation. Instead of building a dense thicket of procedural mandates, the DPDP framework adopts what the Indian government terms the SARAL approach: Simple, Accessible, Rational, and Actionable



[4] **Article 35 (Data Protection Impact Assessment - DPIA) EU GDPR:** Requires an assessment for processing activities likely to result in a high risk to the rights and freedoms of individuals

[5] **Chapter VI (Independent Supervisory Authorities) EU GDPR:** Details the powers and duties of national data protection authorities

[6] **Ministry of Electronics and Information Technology (MeitY):** The authority that notified the finalized DPDP Rules on November 13, 2025

Figure 1: SARAL Framework (DPDP Act 2023)[7]

1. Obligation Triage via Significant Data Fiduciaries (SDFs)

Unlike the GDPR, which applies a largely uniform layer of administrative obligations to all data controllers, the DPDP Act strictly separates routine data processing from high-risk processing. Under Section 10[8], the Central Government designates specific entities as Significant Data Fiduciaries based on the volume of data handled, risk to individual rights, and potential impact on national sovereignty or public order.

The heavy administrative duties such as conducting formal DPIAs, undergoing independent annual audits, and maintaining algorithmic transparency are restricted exclusively to these SDFs (such as social media networks, major e-commerce engines, and large gaming platforms). Ordinary businesses are spared these overhead costs, leaving them free to focus resources on core data security rather than procedural paperwork.

2. The Clean-Slate Scope: Exclusively Digital and Digitalized Data

The DPDP Act bypasses the complex, archaic rules regarding physical filing systems that clutter Western privacy laws. Under Section 3[9], it applies strictly to personal data collected in digital form or collected offline and subsequently digitalized. By excluding purely analogy, non-digital records, the framework avoids dragging informal, paper-based small businesses into an unworkable compliance regime.

3. Stripping Away Regulatory Inflation

The Act completely removes the concept of sensitive personal data categories (e.g., separating health, biometrics, or political orientation into rigid sub-compartments with distinct rules). Instead, it applies a singular, high-standard baseline of protection to all digital personal data. This eliminates the legal hair-splitting and compliance friction that organizations face when trying to classify mixed data sets under European rules.

The Consent Manager Model and Structural Asymmetry

A central flaw of the modern digital economy is the breakdown of the traditional notice-and-consent model. In a system dominated by long, complex user agreements the consent becomes an illusion. Users routinely click Accept simply to bypass digital friction, resulting in a structural asymmetry where Data Fiduciaries hold total informational power over the individual (the Data Principal).

To resolve this imbalance without drowning users in continuous pop-up notifications, India introduced an intermediary infrastructure: the **Consent Manager**.

[7] **SARAL Framework:** The acronym for **S**imple, **A**ccessible, **R**ational, and **A**ctionable, representing the Indian government's design philosophy for the DPDP Act 2023

[8] **Section 10:** Outlines the "Obligation Triage" and the specific duties of Significant Data Fiduciaries (SDFs), DPAPA Act 2023.

[9] **Section 3:** Defines the scope as exclusively digital or digitalized personal data DPDP Act 2023.

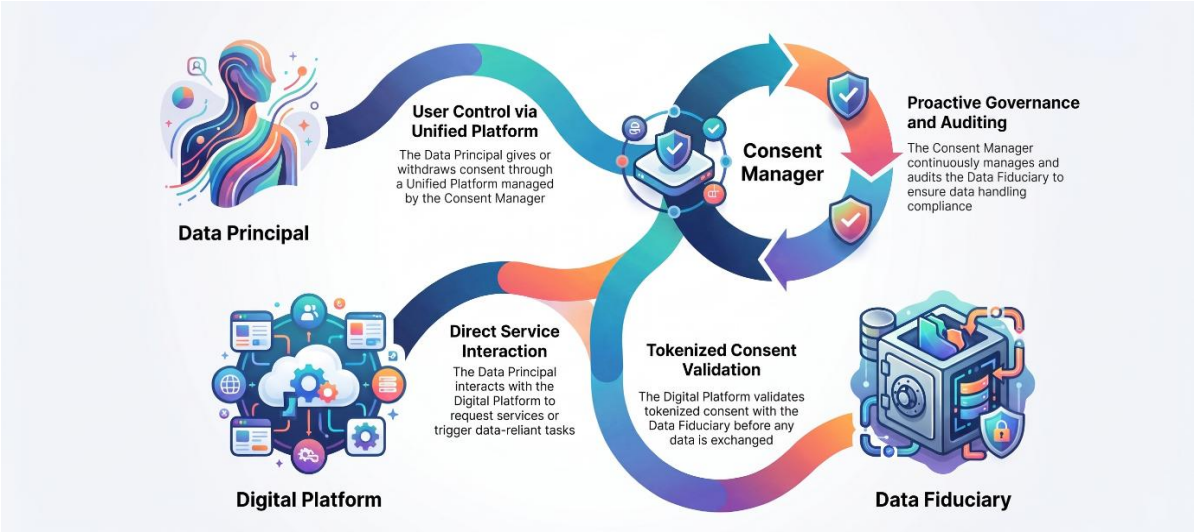


Figure 2: The Decentralized Consent Ecosystem

Under Section 6[10] and Rule 4[11] of the DPDP Rules, Consent Managers are independent, data-blind intermediaries registered and certified by the Data Protection Board of India (DPBI)[12]. They function as an interoperable platform where an individual can give, review, manage and withdraw their data consents across multiple services through a single, clean digital dashboard.

The operational rules established under the Phase II rollout ensure that these managers cannot view the actual underlying personal data; their job is strictly to log and pass along tokenized consent instructions. They are required to hold a minimum net worth of ₹ 2 crores ($200,000) and are barred from subcontracting their core duties or engaging in any conflicts of interest with commercial Data Fiduciaries[13]. By decoupling consent collection from the service delivery platform, the DPDP Act moves the privacy burden away from the individual and giving consumers actual, real-time control over their digital footprint without interrupting their daily user experience.

Cross-Border Transfers and Blacklisting vs. Whitelisting

The international movement of data is essential for modern trade, cloud infrastructure and global technology services. Here is the contrast between the European Union's approach and India's new model is stark. The GDPR relies on a restrictive whitelisting system that based on concept that cross-border data transfers are prohibited unless the recipient country is granted a formal adequacy decision by the European Commission, or the exporting company implements complex legal mechanisms like Standard Contractual Clauses (SCCs)[14] or Binding Corporate Rules (BCRs)[15]. For companies outside the EU, navigating these tools

[10] **Section 6:** Establishes the framework for consent and the use of Consent Managers, DPDP Act 2023.
[11] **Rule 4:** Governing the registration and certification of Consent Managers, DPDP Rules 2025.
[12] **Rule 20:** Mandating the Data Protection Board of India (DPBI) to function as a digital-first office, DPDP Rules 2025.
[13] **Schedule to the Act:** Specifies the penalty scale, including fines up to ₹250 crores for substantive security failures, DPDP Act 2023.
[14] **Article 46 (Transfers Subject to Appropriate Safeguards):** Permits transfers via Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs) in the absence of an adequacy decision, EU GDPR
[15] **Article 47 (Binding Corporate Rules):** specific provision that sets out the criteria for their approval by a competent supervisory authority including their legally binding nature and the specific privacy rights they must guarantee to data subjects, EU GDPR.

involves heavy legal expenses and exposes them to sudden disruptions from judicial rulings, such as the ***Schrems II***[16] decision by the Court of Justice of the European Union.

The DPDP Act turns this approach on its head by adopting a lean, pro-growth blacklisting model under Section 16[17].

By permitting data to flow freely by default, India ensures that its massive technology, business process management (BPM), and SaaS (Software as a Service) sectors can integrate smoothly with global cloud infrastructures. The government keeps the right to step in and block transfers to specific countries based on national security, geopolitical developments, or systemic privacy risks. This negative list model offers a flexible compromise it gives the state necessary regulatory control while sparing the business community continuous compliance costs.

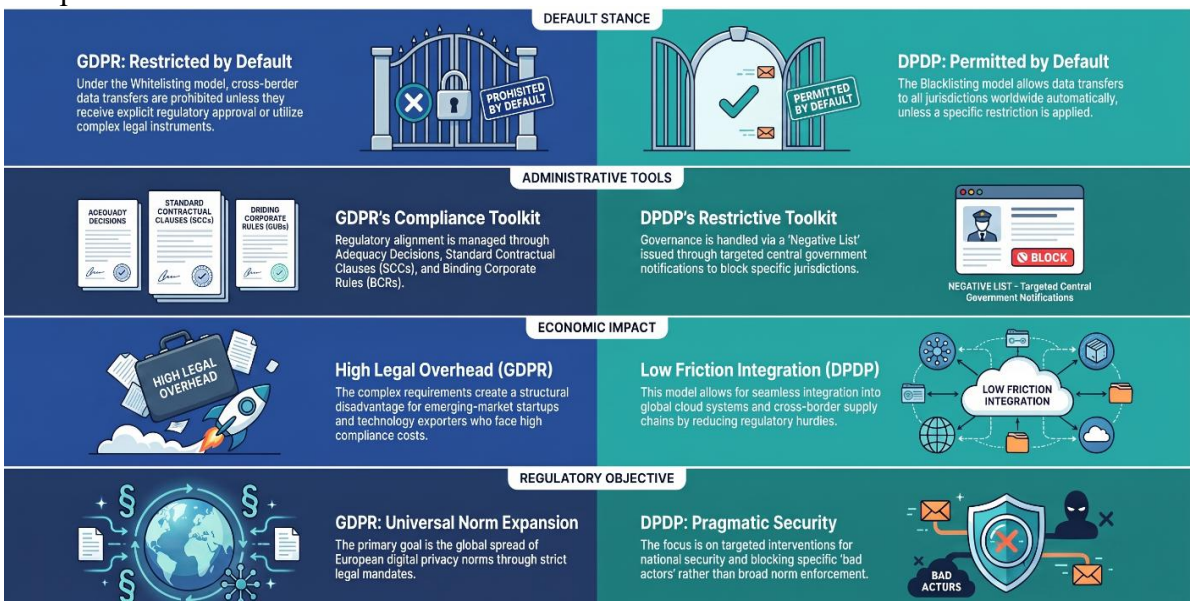


Figure 3: GDPR Whitelisting vs DPDP Blacklisting

The Digital-First Authority and the Death of Proceduralism

Traditional data protection enforcement often gets bogged down in proceduralism focusing heavily on checking compliance forms, reviewing internal policy manuals and inspecting corporate records. This bureaucratic approach regularly leads to severe backlogs, where regulatory bodies spend years investigating process errors rather than fixing actual consumer harms.

The DPDP framework addresses this by pairing strict enforcement with a digital first AND outcome driven administrative setup[18]:

- **The Outcome-Oriented Penalty Scale:** The DPDP Act drops minor fines for administrative or paperwork errors. Instead, under the Schedule to the Act, it saves its highest financial penalties—up to ₹250 crore ($30 million) per incident—for concrete, substantive failures, such as a Data Fiduciary's failure to maintain reasonable security safeguards to prevent an actual data breach.
- **The Digital Office Mandate:** Under Rule 20 of the DPDP Rules, the Data Protection Board of India (DPBI) is legally designed to function as a digital-first office. The entire enforcement process—from filing an individual complaint and presenting digital evidence to

[16] **Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (Schrems II), Case C-311/18**.
[17] **Section 16:** Details the blacklisting model for cross-border data transfers, DPDP Act 2023
[18] Rights-First vs. Economy-First: A Comparative Analysis of the GDPR and India's DPDP Act, Niharika Jaiswal and Dr. Kavya Chandel, Vol. 6, Issue 1, ILE

hearings and issuing orders—is run through an online, tech-enabled platform. This removes geographical barriers for citizens and prevents the slow, paper-heavy delays common in traditional regulatory bodies.

- **The 72-Hour Breach Window and Individual Notification:** Rather than allowing long internal reviews, Rule 7 requires Data Fiduciaries to notify both the DPBI and affected individuals immediately upon becoming aware of a personal data breach, with a detailed follow-up report within 72 hours. This ensures fast public accountability and swift mitigation, focusing attention on managing real-world harms.

By shifting focus away from routine compliance audits and toward preventing actual data exposure, the DPDP framework offers an enforcement model that works efficiently within the fast-moving digital realities of the Global South.

Proposing the Lean Data Governance Framework for Emerging Markets

The implementation of the DPDP Act and its accompanying Rules offers a clear path forward for developing nations looking to move past the rigid confines of the Brussels Effect. This evolution signals the rise of a new regulatory approach: the **Lean Data Governance** framework.

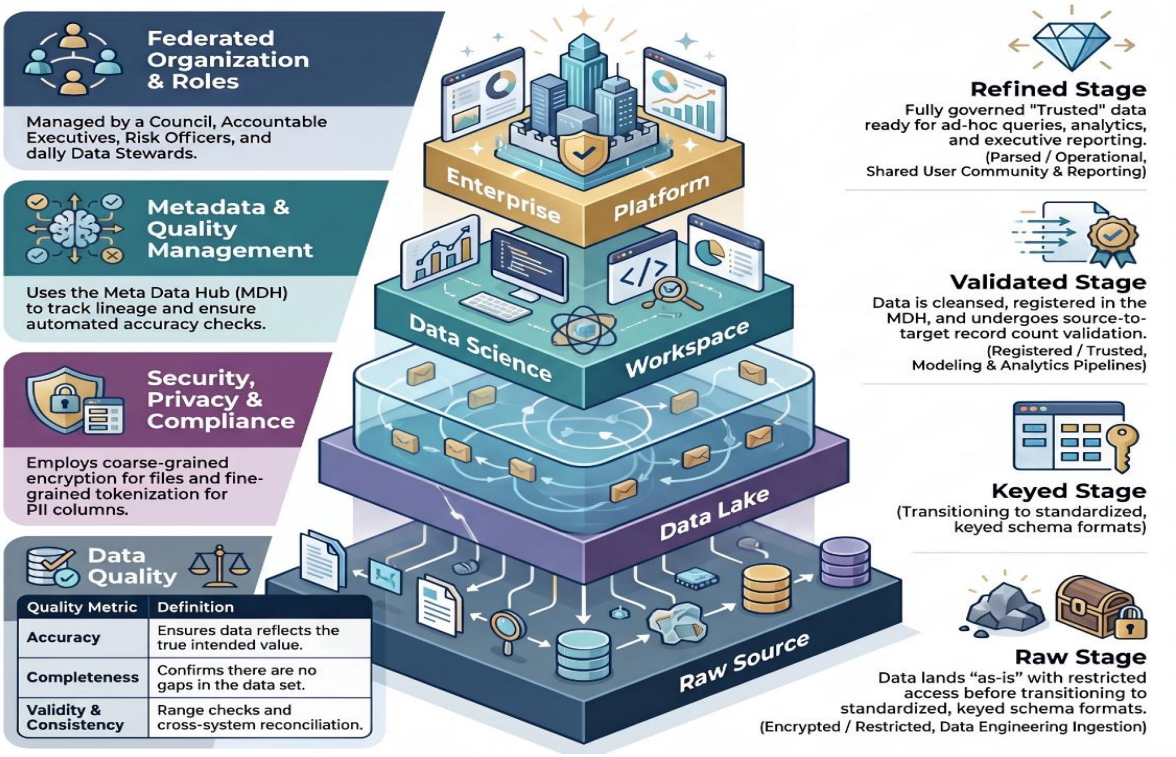


Figure 4: Lean Data Governance Model

This model provides global policymakers with three foundational pillars for designing data laws tailored to emerging economies:

1. **Asymmetric Burden Allocation:** Data laws must drop the one size fits all model. Regulators should tier obligations by market impact, concentrating advanced compliance requirements on large digital platforms while shielding small businesses and local innovators from restrictive overhead.

2. **Interoperable, Tech-Led Intermediaries:** Rather than expecting users to decipher complex legal documents, countries should use simple, technology-driven intermediaries like Consent Managers. Handling privacy through clean, secure software layers makes data control genuinely accessible to diverse and rapidly growing online populations.

3. **Outcome-Focused Enforcement:** Regulators should move away from penalizing formal omissions or internal paperwork gaps. Enforcement must focus squarely on data security and minimizing actual consumer harm, using decisive, transparent penalties for severe breaches to maintain public trust.

Conclusion

The universal hegemony of the European Union's General Data Protection Regulation (GDPR) has officially reached its structural limits. For nearly a decade, the Brussels Effect operated on the presumption that a hyper bureaucratic, process-heavy, and individual-centric framework was the sole viable path to securing data privacy. As this article has demonstrated, the uncritical transplantation of these Eurocentric norms into the Global South has historically resulted in paper compliance that means stifling local innovation hubs, burdening micro, small, and medium enterprises (MSMEs) and failing to protect vulnerable populations navigating steep digital literacy and enforcement gaps.

India's Digital Personal Data Protection (DPDP) Act, alongside its operationalized regulatory architecture, marks a definitive paradigm shift toward **Lean Data Governance**. By replacing complex legal paperwork with textual minimalism, flattening the data taxonomy into a single category of personal data, and pivoting to an agile cross-border blacklist model, India has proven that data protection can be engineered to match market speed. More fundamentally, by embedding enforcement directly into Digital Public Infrastructure (DPI) through the statutory vehicle of data-blind **Consent Managers**, the Indian model moves away from the structural fiction of the Western notice-and-consent model. It shifts the burden of privacy protection off the shoulders of the individual and onto automated, technological systems.

Ultimately, the rise of Lean Data Governance signals the maturity of Global South jurisprudence. Developing and transitional economies across Asia, Africa, and Latin America are no longer required to accept a false choice between unregulated data extraction or restrictive European administration. The Indian framework offers a highly scalable, outcome-oriented blueprint that harmonizes individual information autonomy with state sovereignty and economic dynamism. By prioritizing simplicity, technological enforcement, and asymmetric burden allocation, emerging markets can finally break free from regulatory dependencies and build digital legal systems tailored to their own futures.

Bibliography

1. Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, No. 18, Acts of Parliament, 2016 (India).
2. Bhatt, C., & Burman, A. (2024, February 21). Data protection regulation in the Global South. Carnegie Endowment for International Peace. https://carnegieindia.org/2024/02/21/data-protection-regulation-in-global-south-pub-91717.
3. Bradford, A. (2020). The Brussels effect: How the European Union rules the world. Oxford University Press.
4. Charter of Fundamental Rights of the European Union, 2012/C 326/02.
5. Constitution of India, 1950, Art. 21.
6. Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems (Schrems II), Case C-311/18, ECLI:EU:C:2020:559 (2020).
7. Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
8. Digital Personal Data Protection Rules, 2025 (India) (Notified Nov. 13, 2025).
9. Dubey, S., & Sharma, N. (2026). A comparative legal study of the GDPR and India's Digital Personal Data Protection Act. Journal of Advance & Future Research, 4, 414.

10. Google Spain SL v. Agencia Española de Protección de Datos, Case C-131/12, ECLI:EU:C:2014:317 (2014).
11. Greenleaf, G. (2023). India's Digital Personal Data Protection Act 2023: Comparative analysis with the GDPR. Privacy Laws & Business International Report, 184, 20.
12. Jaiswal, N., & Chandel, K. (2026). Rights-first vs. economy-first: A comparative analysis of the GDPR and India's DPDP Act. Indian Journal of Legal Review, 6, 641.
13. John, S. (2025). The legal architecture of digital public infrastructures: Consent, accountability, and data sovereignty in India's Aadhaar and UPI systems. International Journal of Judicial Science Research Studies, 2.
14. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
15. Justice K.S. Puttaswamy (Retd.) v. Union of India (Aadhaar Judgment), (2018) 1 SCC 809.
16. Kumar, R. (2026, January 28). GDPR vs DPDP: Why GDPR first privacy programs fail in India. Levo.ai. https://www.levo.ai/resources/blogs/gdpr-vs-dpdp-india-privacy-compliance.
17. Kuner, C. (2020). The GDPR as a model for global data protection law. Oxford University Press.
18. Malviya, K., & Singh, E. (2025, November 18). Cross-border data transfers and data localization mandate under the data protection regime. Vidhi Centre for Legal Policy. https://vidhilegalpolicy.in/blog/cross-border-data-transfers-and-data-localization-mandate-under-the-data-protection-regime