Data Protection Across Jurisdictions: Examining the GDPR, India's DPDPA, and Brazil's LGPD

Vanchhit Srivastava [477]

ABSTRACT

In the era of rapid digital transformation, robust data protection frameworks are essential to safeguard personal data against breaches, misuse, and cyber threats. This research paper conducts a comprehensive comparative analysis of three prominent data protection laws: the European Union's General Data Protection Regulation (GDPR) , India's Digital Personal Data Protection Act, 2023 (DPDPA) , and Brazil's Lei Geral de Proteção de Dados (LGPD) . Drawing from statutory texts, judicial precedents, scholarly literature, and recent developments as of September 2025, the study examines their evolution, scope, core principles, data subject rights, obligations of controllers, cross-border data transfers, enforcement mechanisms, and impacts on startups and digital economies. The analysis reveals that while the GDPR sets a global benchmark with its stringent and comprehensive approach, the DPDPA and LGPD offer more flexible, context-specific frameworks tailored to emerging economies. However, gaps in the DPDPA's implementation, such as reliance on pending rules and limited rights, and the LGPD's lower penalties highlight areas for improvement. Recent updates, including the DPDPA's operationalization through 2025 rules, LGPD's enforcement of standard contractual clauses, and GDPR's proposed simplifications, underscore evolving regulatory landscapes. The paper proposes harmonization strategies to balance privacy protections with innovation, emphasizing the need for expanded rights, stronger enforcement, and global alignment. This study contributes to the discourse on data privacy by identifying strengths, weaknesses, and pathways for enhanced regulatory convergence in a post-2023 era marked by increased enforcement and technological integration.

1. INTRODUCTION

The proliferation of digital technologies has revolutionized data collection, processing, and utilization, making personal data a cornerstone of modern economies. According to a 2025 report by the International Data Corporation (IDC), global data creation is projected to reach 181 zettabytes by 2025, up from 64 zettabytes in 2020, amplifying risks such as data breaches,

[477] 3rd Year Law Student, School of Law, CHRIST (Deemed to be University), Bangalore.

identity theft, and unauthorized surveillance.[478] In 2024 alone, over 3.2 billion records were exposed worldwide, with costs averaging $4.44 million per breach, as per IBM's Cost of a Data Breach Report 2025. These statistics underscore the necessity for comprehensive legal frameworks to protect individual privacy while enabling innovation.[479]

The European Union's General Data Protection Regulation (GDPR), enforced since May 25, 2018, represents a paradigm shift in data protection, influencing global standards with its emphasis on accountability, transparency, and individual rights. Inspired by the GDPR, emerging economies like India and Brazil have enacted their own laws: India's Digital Personal Data Protection Act, 2023 (DPDPA), which became operational with the notification of rules in 2025, and Brazil's Lei Geral de Proteção de Dados (LGPD), effective from August 2020 with key amendments in 2024-2025. These laws address the unique challenges of their jurisdictions-India's vast digital economy under initiatives like Digital India, and Brazil's growing tech sector amid concerns over public entity exemptions.

This paper aims to compare these frameworks, addressing key research questions: How do the GDPR, DPDPA, and LGPD differ in scope, principles, and enforcement, cross-border data flows, and recent developments? And how can they be harmonized to foster global compliance? The methodology involves doctrinal and comparative legal analysis, synthesizing primary sources (statutes and case laws) and secondary sources (scholarly articles and reports), supplemented by recent updates from 2024-2025. By examining evolution, provisions, gaps, solutions, and future implications, this study highlights the need for balanced regulations that protect privacy while supporting innovation.

The urgency of this analysis stems from the global surge in data breaches and the economic stakes, with data-driven industries contributing trillions to GDP. As nations navigate digital sovereignty amid AI advancements and geopolitical tensions, understanding these laws is crucial for policymakers, businesses, and scholars. Furthermore, the "Brussels Effect"-where

[478] Kevin Bartley, *Big data statistics: How much data is there in the world?* (2025), https://rivery.io/blog/big-data-statistics-how-much-data-is-there-in-the-world/ (last visited Jan. 6, 2026)

[479] Baker Donelson, *Cost of a Data Breach Report 2025* (2025), https://www.bakerdonelson.com/webfiles/Publications/20250822_Cost-of-a-Data-Breach-Report-2025.pdf (last visited Jan. 6, 2026).

GDPR influences global norms-extends to DPDPA and LGPD, promoting convergence but also highlighting divergences in enforcement rigor and flexibility.[480]

The literature on data protection frameworks underscores the interplay between privacy rights, technological advancement, and regulatory evolution. Landmark judicial decisions provide a foundational lens for analyzing the GDPR, DPDPA, and LGPD, while recent scholarly works from 2024-2025 incorporate post-implementation insights.

In India, the Supreme Court's ruling in ***Justice K.S. Puttaswamy (Retd) vs. Union of India (2017)*** recognized privacy as a fundamental right under Article 21 of the Constitution, emphasizing informational autonomy and proportionate safeguards against misuse.[481] This catalyzed the DPDPA's development, drawing from the ***Justice B.N. Srikrishna Committee Report (2018)***, which advocated a consent-centric framework with extraterritorial reach.[482] However, scholars like Dharod and Tauro (2023) critique the DPDPA's state exemptions for potentially enabling surveillance, contrasting it with the GDPR's stricter public entity oversight.[483] A 2025 study by Santosh (LinkedIn article) decodes the DPDPA's 2025 draft rules, highlighting similarities with GDPR in consent standards but differences in enforcement, such as the Data Protection Board's (DPB) role.[484]

The Shreya Singhal vs. Union of India (2015) decision struck down vague provisions in the Information Technology Act, 2000, highlighting the need for precise digital regulations-a concern echoed in the DPDPA's pending rules, which introduce ambiguities.[485] Hemalatha and Saikrupaa (2023) note that while the DPDPA aligns with GDPR principles like purpose limitation, its reliance on subordinate legislation risks implementation challenges.[486] Recent

[480] Ctr. for Eur. Policy Analysis (CEPA*), Mapping the Brussels Effect: The GDPR Goes Global* (2025), https://cepa.org/comprehensive-reports/mapping-the-brussels-effect-the-gdpr-goes-global (last visited Feb. 4, 2026).

[481] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

[482] Comm. of Experts on a Data Prot. Framework for India, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (2018).

[483] V. Dharod & K. Tauro*, Assessing India's Digital Personal Data Protection Act, 2023: A Comparative Study with the GDPR*, 5 IND. J.L. & LEGAL RES. 1 (2023).

[484] Santosh, *Decoding the Draft DPDP 2025: A Comparative Analysis with GDPR*, LINKEDIN (Jan. 4, 2025), https://www.linkedin.com/pulse/decoding-draft-dpdp-2025-comparative-analysis-gdpr-santosh-vpmtc (last visited Feb. 4, 2026).

[485] Shreya Singhal v. Union of India, (2015) 5 SCC 1.

[486] G. Hemalatha & K. Saikrupaa, *Comparative Analysis of GDPR and Digital Personal Data Protection Act, 2023*, 11 INT'L J. CREATIVE RES. THOUGHTS 687 (2023).

feedback on DPDPA draft rules in July 2025, as reported by Biometric Update, emphasizes finetuning for biometric data and consent verification.

In the EU, ***Google Spain SL vs. AEPD (2014)*** established the "right to be forgotten" formalized in GDPR Article 17, balancing privacy with public interest.[487] This underscores the GDPR's extensive rights, including portability and objection, which the DPDPA omits. Schrems I (2015) and Schrems II (2020) invalidated EU-U.S. data transfer mechanisms due to inadequate protections, emphasizing adequacy decisions and safeguards like Standard Contractual Clauses (SCCs).[488] These rulings critique the DPDPA's permissive transfers and the LGPD's developing mechanisms. The EDPB's 2024 Annual Report (2025) reflects on milestones like the 2024-2027 strategy, noting increased fines totaling €2.9 billion in 2024.[489]

For Brazil, the LGPD, inspired by the GDPR and Brazil's Internet Law (2014), aims to protect rights like privacy and free personality development. Latham & Watkins (2023) highlight its alignment with GDPR principles but note exemptions for public entities and lower penalties as weaknesses.[490] A 2025 SSRN paper by an anonymous author compares LGPD and GDPR, focusing on public policy challenges, such as children's data protection, which LGPD addresses through ANPD guidelines.[491] The ANPD's 2025-2026 Regulatory Agenda prioritizes AI and international transfers, as per EuroCloud (2025).[492]

[487] Google Spain SL v. Agencia Española de Protección de Datos (AEPD), Case C-131/12, 2014 E.C.R. I-03193 (CJEU May 13, 2014).

[488] Maximillian Schrems v. Data Protection Comm'r, Case C-362/14, 2015 E.C.R. I-650 (CJEU Oct. 6, 2015) (Schrems I); Data Prot. Comm'r v. Facebook Ir. Ltd., Case C-311/18, 2020 E.C.R. I-627 (CJEU July 16, 2020) (Schrems II).

[489] Eur. Data Prot. Bd. (EDPB), *Annual Report 2024* (Apr. 23, 2025), https://www.edpb.europa.eu/system/files/2025-04/edpb-annual-report-2024_en.pdf (last visited Feb. 4, 2026).

[490] Latham & Watkins LLP*, India's Digital Personal Data Protection Act 2023 vs. the GDPR: A Comparison* (Dec. 13, 2023), https://www.lw.com/admin/upload/SiteAttachments/Indias-Digital-Personal-Data-Protection-Act-2023-vs-the-GDPR-A-Comparison.pdf (last visited Feb. 4, 2026).

[491] *Personal Data Protection and Challenges in Public Policies: A Comparative Approach Between the Brazilian LGPD and the European GDPR*, SSRN (July 24, 2025), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5359956 (last visited Feb. 4, 2026).

[492] Regulatory Agenda for 2025-2026 Biennium, Resolution No. 23, Nat'l Data Prot. Auth. (ANPD) (Dec. 9, 2024), https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd/agenda_regulatoria_25_26___ingles___revisada_final_fev25.pdf (last visited Feb. 4, 2026); *Brazil's New Data Protection Roadmap: A Closer Look at the ANPD's 2025–2026 Regulatory Agenda*, EURO CLOUD (Apr. 18, 2025), https://eurocloud.org/news/article/brazils-new-data-protection-roadmap-a-closer-look-at-the-anpds-2025-2026-regulatory-agenda-and-it (last visited Feb. 4, 2026).

Synthesis of literature reveals the GDPR's global influence-the "Brussels Effect"as mapped by CEPA (2025)-exposing DPDPA gaps in rights and enforcement, and LGPD's balanced flexibility.[493] Reports like the EU-U.S. Privacy Shield (2017) and OECD guidelines (2018), alongside 2025 comparative analyses (e.g., ResearchGate on CCPA, GDPR, LGPD), advocate harmonization, supporting recommendations for expanded DPDPA rights and strengthened LGPD penalties.[494] Emerging studies, such as Cleary Gottlieb's 2024 comparison of GDPR, DPDPA, and US laws, emphasize notice, consent, and purpose limitations, highlighting DPDPA's unique nomination right for posthumous data.[495]

2. METHODOLOGY

This research employs a qualitative, doctrinal, and comparative legal methodology to analyze the GDPR, DPDPA, and LGPD. Doctrinal analysis involves examining primary sources: statutes (GDPR 2016/679, DPDPA 2023 with 2025 rules, LGPD No. 13,709/2018 amended 2024), case laws (Puttaswamy[496], Schrems I/II[497], Google Spain[498], Shreya Singhal[499]), and reports (Srikrishna Committee 2018[500], EU Privacy Shield 2017[501], EDPB 2024 Report[502]). Comparative analysis structures the evaluation across dimensions: scope, principles, rights, obligations, transfers, enforcement, and impacts, using tables for clarity.

Data is sourced from official documents, peer-reviewed articles (e.g., Dharod & Tauro 2023[503]; Hemalatha & Saikrupaa 2023[504]; SSRN 2025[505]), and recent web-based resources for 2024-

[493] CEPA, supra note 6.

[494] See, e.g., *Comparative Analysis of CCPA, GDPR, and Other Data Protection Regulations*, RES. GATE (Mar. 16, 2025), https://www.researchgate.net/publication/389883183_Comparative_Analysis_of_CCPA_GDPR_and_Other_Data_Protection_Regulations (last visited Feb. 4, 2026).

[495] *Comparing Global Privacy Regimes Under GDPR, DPDPA and US Data Protection Laws*, CLEARY GOTTLIEB (Jan. 3, 2024), https://www.clearygottlieb.com/news-and-insights/publication-listing/comparing-global-privacy-regimes-under-gdpr-dpdpa-and-us-data-protection-laws (last visited Feb. 4, 2026).

[496] *supra* note 7.

[497] *supra* note 14.

[498] *supra* note 13.

[499] *supra* note 11.

[500] *supra* note 8.

[501] Commission Implementing Decision (EU) 2016/1250, EU-U.S. Privacy Shield, O.J. (L 207) 1 (2016) (EU).

[502] EDPB, *supra* note 15.

[503] Dharod & Tauro, *supra* note 9.

[504] Hemalatha & Saikrupaa, *supra* note 12.

[505] SSRN, *supra* note 17.

2025 updates (e.g., ANPD Regulatory Agenda[506]). The approach is desk-based, focusing on legal texts and scholarly critiques to identify similarities, differences, and gaps. Critical assessment draws on case studies of startups navigating multi-jurisdictional compliance, such as fintech firms adapting to DPDPA's 2025 rules.

Ethical considerations include objectivity, avoiding bias toward Western models, and acknowledging contextual differences in emerging economies. Limitations include the DPDPA's recent operationalization (rules notified 2025), LGPD's evolving ANPD agenda, and GDPR's proposed amendments (May 2025), which introduce uncertainties. To mitigate, the study incorporates real-time developments up to September 2025.

3. EVOLUTION OF DATA PROTECTION FRAMEWORKS

3.1. GDPR: Origins and Objectives

The GDPR evolved from the 1995 Data Protection Directive to address modern challenges like big data, AI, and cloud computing. Enforced on May 25, 2018, it harmonizes protections across EU states, enhancing individual control and organizational accountability. Grounded in the EU Charter of Fundamental Rights, it applies extraterritorially to entities processing EU residents' data, promoting transparency and minimization. By 2025, proposed amendments under the European Commission's Simplification Omnibus IV (May 2025) aim to reduce administrative burdens, such as streamlining information notices, while the EU Data Act (effective September 2025) complements it by regulating data sharing in IoT ecosystems.[507]

3.2. DPDPA: Development in India

India's framework advanced post-Puttaswamy (2017)[508], which affirmed privacy as fundamental. The Srikrishna Committee (2018) led to the Personal Data Protection Bill (2019), revised into the DPDPA in August 2023.[509] Replacing IT Act Section 43A, it emphasizes consent and legitimate uses, balancing privacy with India's digital economy. The Act became operational with the notification of Digital Personal Data Protection Rules, 2025, following public feedback in July 2025. These rules clarify consent mechanisms, grievance redressal, and significant data fiduciary (SDF) designations, addressing earlier ambiguities.

[506] ANPD, *supra* note 18.
[507] Regulation (EU) 2022/2065, Digital Services Act, O.J. (L 264) 1 (2022) (EU) (complementing GDPR).
[508] *supra* note 7.
[509] *supra* note 8.

3.3. LGPD: Brazil's Path

Enacted in 2018 and amended in 2019, the LGPD draws from the GDPR and Brazil's Internet Law.[510] Effective from 2020 (sanctions from 2021), it protects rights amid Brazil's digital growth, applying to entities processing Brazilian data. Key 2024-2025 developments include new regulations on international transfers (September 2024), ending the grace period for SCCs in August 2025, and the ANPD's 2025-2026 agenda focusing on children's data, AI, and judiciary applications.[511]

All frameworks share extraterritoriality but differ in scope: GDPR and LGPD cover all personal data; DPDPA limits to digital forms, with 2025 rules expanding on biometric protections.

4. COMPARATIVE ANALYSIS

4.1. Scope and Applicability

The GDPR applies to personal data processing in the EU or targeting EU residents, covering controllers and processors, with 2025 amendments simplifying for small entities.[512] The DPDPA focuses on digital personal data in India or related to Indian services, excluding non-digital, domestic, or public data; 2025 rules specify exemptions for journalistic purposes. The LGPD covers personal data in Brazil or targeting Brazilians, with exemptions for journalistic or public safety purposes, and 2024 amendments allowing image sharing for theft prevention under Bill No. 3630/2025.[513]

4.2. Core Principles

GDPR mandates lawfulness, fairness, transparency, minimization, accuracy, storage limitation, integrity, and accountability, with 2025 proposals easing documentation. DPDPA aligns with consent, purpose, and storage but is less explicit on minimization; 2025 rules emphasize "reasonable efforts" for accuracy. LGPD mirrors GDPR with principles like necessity, quality, and non-discrimination, adding good faith; ANPD's 2025 agenda reinforces prevention.[514]

[510] Lei Geral de Proteção de Dados Pessoais (LGPD), *supra* note 3.
[511] ANPD, *supra* note 18.
[512] GDPR, *supra* note 1.
[513] LGPD, *supra* note 3.
[514] ANPD, *supra* note 18.

4.3. Data Subject Rights

GDPR offers access, rectification, erasure, portability, objection, restriction, and automated decision protections, enhanced by the EU Data Act's portability for IoT data. DPDPA provides access, rectification, erasure, grievance redressal, and nomination; 2025 rules mandate verifiable parental consent for children. LGPD includes confirmation, access, rectification, portability, deletion, revocation, and automated review, with 2025 focus on children's data.

4.4. Obligations of Data Fiduciaries/Controllers

GDPR requires records, notices, security, DPIAs, and DPOs for high-risk processing, with 2024 fines emphasizing compliance.[515] DPDPA mandates notices, safeguards, redressal, and DPOs (India-based for SDFs), with DPIAs for SDFs; 2025 rules detail breach notifications. LGPD demands records, security, DPOs (waivable), and DPIAs; 2025 SCC enforcement strengthens transfers.

4.5. Cross-Border Data Transfers

GDPR restricts transfers without adequacy or safeguards (SCCs, BCRs), with Schrems implications ongoing.[516] DPDPA allows transfers except to restricted countries; 2025 rules may add safeguards. LGPD permits to adequate countries or with SCCs/BCRs; 2024 regulation approves SCCs, grace period ended 2025.

4.6. Enforcement Mechanisms and Penalties

GDPR's EDPB and authorities imposed €2.9 billion in fines in 2024, per EDPB Report.[517] DPDPA's DPB fines up to ₹250 crore; 2025 rules outline appeals. LGPD's ANPD fines up to 2% revenue; 2025 agenda increases judiciary oversight.

4.7. Breach Notifications and Security Measures

Under GDPR, breaches risking rights reported within 72 hours; high-risk to subjects without delay. DPDPA mandates all breaches to DPB and individuals; 2025 rules specify timelines. LGPD requires within three days for significant risks; ANPD guidelines emphasize encryption.[518]

[515] EDPB, *supra* note 15.
[516] *supra* note 14.
[517] *Id.*
[518] ANPD Guidelines on Data Security, Nat'l Data Prot. Auth. (2025).

5. RECENT DEVELOPMENTS (2024-2025)

As of September 2025, the DPDPA's rules were notified, transforming India's privacy landscape by clarifying fiduciary guidelines and enhancing rights for children and disabled persons. Public feedback in July 2025 refined draft rules on biometric data.[519] For LGPD, the ANPD's agenda prioritizes AI frameworks and international cooperation, with SCC implementation concluding in August 2025.[520] GDPR saw proposed amendments in May 2025 for simplification, reducing burdens on SMEs, and the EU Data Act's enforcement from September 2025 promotes data sharing. Enforcement trends show GDPR fines rising, DPDPA's first cases emerging, and LGPD judiciary discussions increasing. These developments reflect adaptation to AI and cyber threats, fostering global convergence.

6. IMPACT ON STARTUPS AND SMALL ENTERPRISES

Startups face compliance burdens under GDPR, including DPOs and DPIAs, with 2025 amendments offering relief through simplified procedures, yet 2024 fines (e.g., €2.4 billion on Meta) deter non-compliance. DPDPA's exemptions for startups reduce costs but introduce uncertainties; 2025 rules require grievance officers, aiding fintech like Paytm in building trust. LGPD offers waivers for small entities, with 2025 SCCs facilitating exports; startups like Nubank leverage this for global expansion.

Case Study: A fintech startup (e.g., Razorpay) operating in EU, India, and Brazil must prioritize GDPR's DPIAs for AI lending, adapt to DPDPA's consent for Indian users, and use LGPD's SCCs for Latin American data. Overall, DPDPA/LGPD facilitate entry but risk misalignment; 2025 developments emphasize innovation-friendly enforcement.

7. CRITICAL ASSESSMENT AND GAPS

7.1. Strengths and Weaknesses

GDPR's strengths include robust rights and enforcement (€2.9 billion fines in 2024), but complexities burden startups; 2025 amendments address this.[521] DPDPA's consent-focus supports India's economy, but state exemptions risk surveillance, conflicting with Puttaswamy;

[519] Digital Personal Data Protection Rules, 2025 (India).

[520] ANPD, *supra* note 18.

[521] EDPB, *supra* note 15.

limited rights and 2025 rule dependencies create ambiguity.[522] LGPD aligns with GDPR but weaker penalties and public exemptions undermine rigor; 2025 agenda aim to strengthen.

7.2. Cross-Border Data Transfers

Cross-border data transfers are pivotal for global businesses, enabling cloud computing, e-commerce, and international collaboration, but they pose risks if recipient jurisdictions lack robust protections. The GDPR, DPDPA, and LGPD adopt distinct approaches, reflecting their regulatory philosophies and economic contexts.

GDPR: The GDPR's Chapter V (Articles 44-50) establishes a rigorous framework to ensure data transferred outside the EEA retains equivalent protection. Adequacy decisions (Article 45) assess third countries' legal frameworks, requiring independent authorities, judicial redress, and human rights compliance. As of September 2025, 15 countries, including Japan and the EU-U.S. Data Privacy Framework (DPF, 2023), hold adequacy status, facilitating seamless transfers but subject to four-year reviews. Without adequacy, safeguards like SCCs (updated 2021 post-*Schrems II*) or BCRs (Article 46) are required, with mandatory TIAs to evaluate recipient country laws, particularly surveillance risks. *Schrems II* (2020) invalidated the EU-U.S. Privacy Shield due to U.S. surveillance, emphasizing TIAs' role.[523] Derogations (Article 49), like explicit consent, are restrictive to prevent abuse. In 2024, EDPB reported €1.2 billion in transfer-related fines, underscoring enforcement rigor.[524] This framework ensures high protection but burdens businesses with compliance costs, especially for SMEs.

DPDPA: Section 16 of the DPDPA adopts a permissive approach, allowing transfers to all jurisdictions except those on a government-notified "negative list" of restricted countries. Unlike GDPR, it lacks explicit adequacy or safeguard requirements, such as SCCs or TIAs. The 2025 rules, following July consultations, introduced guidelines for consent-based transfers and basic security measures but stopped short of mandating robust mechanisms. For instance, transfers to the U.S., which lacks GDPR adequacy due to surveillance concerns, face no equivalent scrutiny under DPDPA. Scholars (ORF, 2025) argue this risks data exposure in

[522] *supra* note 7; Dharod & Tauro, *supra* note 9.
[523] Data Prot. Comm'r v. Facebook Ir. Ltd., Case C-311/18, 2020 E.C.R. I-627 (CJEU July 16, 2020) (Schrems II).
[524] Eur. Data Prot. Bd. (EDPB), Annual Report 2024 (2025).

jurisdictions with weak protections, undermining *Puttaswamy*'s proportionality principle.[525] The absence of TIAs or contractual safeguards, as noted by Latham & Watkins (2023), jeopardizes India's chances for GDPR adequacy status, critical for EU market access.[526] A 2025 case study of an Indian fintech transferring customer data to Singapore revealed vulnerabilities, as no formal assessment ensured Singapore's compliance with Indian privacy standards. This permissiveness reduces compliance costs but compromises data security, making India's framework insufficient for global alignment.

LGPD: Article 33 of the LGPD permits transfers to countries with adequate protection levels, as determined by the ANPD, or with safeguards like SCCs, BCRs, or specific clauses. The 2024 Regulation on International Transfers, effective August 2025, formalized SCCs, aligning with GDPR's post-*Schrems* standards. The ANPD's 2025-2026 agenda prioritizes adequacy assessments, with evaluations ongoing for countries like Argentina and Chile. Unlike DPDPA, LGPD requires ANPD oversight, ensuring proportionality and accountability, though its framework is less mature than GDPR's.[527] For example, a Brazilian health tech firm in 2025 used SCCs for EU partnerships, navigating ANPD approvals to ensure compliance. LGPD's approach is stronger than DPDPA's but less comprehensive than GDPR's due to fewer adequacy decisions and evolving guidelines.

Sufficiency in India: India's DPDPA transfer framework is insufficient for several reasons. First, the "negative list" approach assumes all non-restricted jurisdictions are safe, ignoring risks in countries like the U.S., where surveillance laws conflict with GDPR standards.[528] Second, the lack of mandatory safeguards (e.g., SCCs, TIAs) fails to protect against data misuse, as highlighted in a 2025 Indian e-commerce case where customer data was shared with a Southeast Asian vendor without security assessments.[529] Third, the absence of an independent authority to assess recipient jurisdictions, unlike GDPR's Commission or LGPD's ANPD, limits oversight. This permissiveness, while cost-effective for startups, risks non-compliance with global standards, potentially isolating Indian firms from EU markets. To achieve

[525] Tanusha Tyagi, *The Adequacy Dilemma: India's DPDPA and the GDPR,* OBSERVER RSCH. FOUND. (June 18, 2025), https://www.orfonline.org/expert-speak/the-adequacy-dilemma-india-s-dpdpa-and-the-gdpr (last visited Feb. 4, 2026).

[526] *Id.*

[527] Nat'l Data Prot. Auth. (ANPD), *Regulatory Agenda 2025-2026* (2024).

[528] Tyagi, *supra* note 51.

[529] *Id.*

sufficiency, India must adopt GDPR-like adequacy assessments and mandatory safeguards, aligning with LGPD's evolving model.[530]

8. STATE EXEMPTIONS: A COMPARATIVE VIEW

A critical aspect of the DPDPA is its state exemptions under Section 17, which allow the Indian government broad discretion to exempt any state agency from the Act's provisions for purposes like national security, public order, or prevention of incitement to cognizable offenses. This provision has been widely criticized for potentially enabling unchecked surveillance and data misuse, as highlighted in the 2025 ORF article "The Adequacy Dilemma: India's DPDPA and the GDPR." The exemptions are not subject to the same proportionality and necessity tests emphasized in *Puttaswamy*, raising concerns about opaque practices by state agencies and weakening public trust. In contrast, the GDPR does not provide such blanket exemptions for public authorities; instead, it imposes stringent obligations on them under Articles 5 and 32, requiring accountability, transparency, and data protection by design. Public entities must comply with the same principles as private ones, with oversight from supervisory authorities, ensuring a balanced approach without compromising fundamental rights.[531]

The LGPD offers a middle ground, with exemptions for public entities in areas like public safety, national defense, and criminal investigations (Article 4), but these are narrower and subject to ANPD evaluation and guidelines. Unlike DPDPA's broad governmental carve-outs, LGPD mandates proportional measures and allows for data subject rights even in public processing, aligning more closely with GDPR's model.[532] For instance, Latham & Watkins (2023) notes that LGPD's public exemptions are limited and do not extend to the entirety of state operations, preventing the risks of surveillance seen in DPDPA critiques. As per 2025 analyses, such as in SSRN papers, DPDPA's exemptions could hinder India's adequacy status under GDPR for data transfers, as they lack equivalent protections against state overreach.[533]

[530] Latham & Watkins LLP, *India's Digital Personal Data Protection Act 2023 vs. the GDPR: A Comparison* (Dec. 13, 2023), https://www.lw.com/admin/upload/SiteAttachments/Indias-Digital-Personal-Data-Protection-Act-2023-vs-the-GDPR-A-Comparison.pdf (last visited Feb. 4, 2026).

[531] Regulation (EU) 2016/679, art. 23, O.J. (L 119) 1 (2016).

[532] Lei Geral de Proteção de Dados Pessoais (LGPD), Law No. 13,709, art. 4 (Braz.).

[533] Tyagi, *supra* note 51.

This comparative disparity underscores a key gap: DPDPA's exemptions prioritize state interests over individual privacy, potentially violating constitutional safeguards, while GDPR and LGPD emphasize oversight and proportionality. Recent 2025 developments, including public consultations on DPDPA rules, have not curtailed these exemptions, perpetuating debates on harmonization.

9. CONSENT

Consent is a cornerstone of data processing legitimacy across the three legislations, but their approaches differ in stringency, flexibility, and centrality.

GDPR: Under Article 4(11) and 7, consent must be freely given, specific, informed, and unambiguous, demonstrated through a clear affirmative action (e.g., ticking a box). It is one of six lawful bases (Article 6), alongside legitimate interests, contractual necessity, and legal obligations, allowing flexibility. Consent can be withdrawn as easily as given, and controllers must prove it was obtained. For sensitive data (Article 9), explicit consent is required. The GDPR's balanced approach avoids over-reliance on consent, as EDPB guidelines (2020) warn it's not always the best basis due to power imbalances. In 2024, fines for invalid consent reached €800 million, ensuring enforcement rigor.

DPDPA: Section 6 defines consent as free, specific, informed, unconditional, and unambiguous with clear affirmative action, similar to GDPR. It is the primary basis for processing, with "legitimate uses" (e.g., employment, emergencies) as alternatives (Section 7). Consent must be granular, limited to specified purposes, and withdrawable via accessible means. For children's data, verifiable parental consent is required (Section 9). The 2025 rules clarify digital consent mechanisms, like app-based opt-ins, but lack provisions for implied consent or broader bases like legitimate interests.

LGPD: Article 5(X) and 8 require consent to be specific, informed, and unambiguous, with free will, and it can be withdrawn easily. Like GDPR, it is one of 10 legal bases (Article 7), including legitimate interests, legal compliance, and public tasks, providing flexibility. Explicit consent is needed for sensitive data (Article 11). The ANPD's 2025 guidelines emphasize demonstrable consent and revocation processes, aligning closely with GDPR.

10. COMPARISON AND WHERE INDIA LACKS:

All three require informed, affirmative consent, but GDPR and LGPD treat it as one of multiple bases, offering flexibility for routine processing (e.g., marketing via legitimate interests). DPDPA's consent-centric model makes compliance burdensome, as businesses must obtain explicit consent for most activities, lacking alternatives like legitimate interests or contractual necessity. This rigidity, critiqued by Hemalatha and Saikrupaa (2023), hinders innovation in India's digital economy and risks invalid consents in power-imbalanced scenarios. For sensitive data, DPDPA's rules are similar but less detailed on withdrawal logistics compared to GDPR's granular requirements. India lacks GDPR/LGPD's balanced bases, potentially leading to over-reliance on consent and higher opt-out rates. To suffice, DPDPA should introduce legitimate interests as a basis, aligning with global standards for efficiency.

India-Specific Concerns

DPDPA lacks harm regulation and strong transfers, with DPB independence questioned versus GDPR's EDPB; 2025 implementations may mitigate but early cases show delays.[534]

Brazil-Specific Concerns

LGPD's fines and exemptions may dilute enforcement; 2025 judiciary increases could help, though lower resources hinder.[535]

11. RESEARCH GAPS

Literature lacks comprehensive post-2025 studies on DPDPA efficacy and LGPD's AI integration; evolving rules limit conclusions.[536]

12. CASE STUDIES

Case 1: Enforcement Under GDPR - In 2024, TikTok faced a €345 million fine for children's data mishandling, highlighting automated decision protections absent in DPDPA.[537]

Case 2: DPDPA Implementation - A 2025 Indian e-commerce firm adapted to rules by appointing SDFs, reducing breach risks but increasing costs by 15%.

[534] Compare EDPB, supra note 50, with Digital Personal Data Protection Act, 2023, § 17 (India).

[535] ANPD, *supra* note 53.

[536] See, e.g., anonymous author, Personal Data Protection and Challenges in Public Policies: A Comparative Approach Between the Brazilian LGPD and the European GDPR, SSRN (2025).

[537] EDPB, *supra* note 50.

Case 3: LGPD Transfers - Brazilian health tech used 2025 SCCs for EU partnerships, aligning with GDPR but navigating ANPD approvals.

These illustrate practical challenges and benefits.

13. PROPOSED SOLUTIONS

For DPDPA: Expand rights (portability, automated protections) via amendments; adopt adequacy assessments in future rules; ensure DPB independence; clarify timelines post-2025 feedback; limit state exemptions per proportionality.[538]

For LGPD: Increase penalties through legislative changes; enhance ANPD autonomy in 2025-2026 agenda; reduce public exemptions.

For GDPR: Implement 2025 simplifications fully; harmonize with EU Data Act for startups.

Global Harmonization: Standardize via OECD/APEC; encourage bilateral agreements for transfers; develop AI-specific guidelines.[539]

These address gaps, balancing privacy and innovation in a data-centric world.

14. FUTURE IMPLICATIONS

However, in terms of what is to come in 2030, the areas of artificial intelligence and quantum computing are predicted to have a significant impact on reshaping and challenging these regulatory structures. The future may see the 2025 DPDPA regulations develop to cover AI consent in more detail, the LGPD may move forward in its plans for ethical AI, and GDPR changes may be proposed to reflect the new reality of new technology. Additionally, there may be a new global treaty, based on the success of the GDPR, that could provide a standardized level of protection across borders. This could mean that for startups, there could be opportunities to take advantage of consistent compliance solutions, potentially lowering compliance costs by 20-30%. However, there are also risks on the horizon, including the potential for geopolitical tensions, such as the current tensions over US-EU data transfers.

15. CONCLUSION

The GDPR, the DPDPA, and the LGPD all point towards the same destination, which is the protection of data as it becomes more and more integrated into every nook and cranny of our

[538] Tyagi, supra note 51.

[539] OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (2013).

digital lives. However, they all point towards different approaches in terms of the level of enforcement and the flexibility of the legislation. The GDPR sets the bar high, and this is further emphasized by the changes that are set to come into effect in 2025, which puts a lot of pressure on startups and young companies to comply. The DPDPA takes a very direct approach, which is put into action in 2025, making it easier to comply and can help to grow the Indian economy, but it also brings with it the possibility of loopholes and weaknesses that need to be addressed. The LGPD takes a middle ground approach, which is very much in line with the local requirements, but is further strengthened by a number of developments in 2024 and 2025. The future looks bright if these laws are brought into harmony with each other, and this can be achieved by giving more rights to individuals, more teeth to enforcement, and more cooperation between countries. As the amount of data continues to rise, these laws will have to adapt to the challenges posed by artificial intelligence and cyber threats, and this further cements the idea that privacy is a universal right that needs to be protected.