E-ISSN No : 2581-6195 | Volume : 9 | Special Issue | May 2026

DATA PRIVACY IN FINTECH: GDPR VS. INDIA'S DPDP ACT — A COMPARATIVE ANALYSIS

Mr. Sangmesh Ainapur[1], Shradha Andur[2], Shradha K[2]

ABSTRACT

The rapid growth of FinTech has changed the way people use financial services, while also increasing concerns about data privacy and security. This study compares the European Union's GDPR and India's Digital Personal Data Protection (DPDP) Act in the context of FinTech operations. Using data from legal documents, regulatory reports, and academic studies from 2016–2024, the article examines key areas such as consent, data processing, compliance requirements, enforcement, and cross-border data transfer. The study finds that although both laws focus on protecting personal data, the GDPR follows a stricter rights-based approach, whereas India's DPDP Act takes a more flexible and sovereignty-focused approach. The paper also highlights the compliance challenges faced by FinTech firms operating in both regions and suggests policy recommendations for better alignment with global data protection standards.

KEYWORDS: GDPR, DPDP Act, Data Privacy, FinTech, Personal Data Protection, Regulatory Compliance, Data Localisation, Consent Framework, Cross-Border Data Transfer, Financial Technology, India, European Union, Data Fiduciary, Right to Erasure, Algorithmic Accountability

[1] Asst Prof., Dept. of MBA, Lingaraj Appa Engineering College, Bidar

[2] Student, Department of Master of Business Administration, Guru Nanak Dev Engineering College, Bidar, Karnataka, India

How to Cite:
Mr. Sangmesh Ainapur, Shradha Andur & Shradha K (2026), Data Privacy In Fintech: Gdpr Vs. India's Dpdp Act — A Comparative Analysis, International Educational Journal of Science & Engineering (IEJSE),Vol: 9, Special Issue, May 2026 588-593

1.INTRODUCTION

In the digital economy, data has become the foundation of FinTech services such as digital payments, online lending, and personalised banking. While these innovations improve financial access and convenience, they also raise concerns about privacy, data misuse, and security. To address these issues, the European Union introduced the GDPR in 2018, while India enacted the Digital Personal Data Protection (DPDP) Act in 2023. Both laws aim to protect personal data, but they differ in approach and enforcement. As FinTech companies increasingly operate across borders, understanding and complying with these frameworks has become essential for ensuring data security and customer trust.

2. LITERATURE REVIEW

The existing literature highlights that data privacy and protection have become central issues in the rapidly growing FinTech sector, where companies rely heavily on personal and financial data for services such as digital payments, lending, robo-advisory, and AI-based financial solutions. Early scholars like Alan Westin (1967) defined privacy as an individual's right to control personal information, while Daniel Solove (2006) explained how digital technologies create multiple forms of privacy risks, including data collection, profiling, and misuse. These ideas form the foundation of modern data protection laws such as the GDPR and India's DPDP Act.

Several studies have examined the impact of the GDPR on digital businesses and financial services. Paul Voigt and Axel von dem Bussche (2017) observed that the GDPR introduced strict compliance standards, strong enforcement mechanisms, and extraterritorial

Research Paper

applicability, making it a global benchmark for data protection. Similarly, Jan Philipp Albrecht (2016) argued that the GDPR was designed to strengthen consumer trust in the digital economy through accountability and transparency.

In the Indian context, B. N. Srikrishna (2018) emphasised the need to balance individual privacy rights with business innovation and state interests while framing India's data protection law. Later studies by Bhatia and Kak (2020) noted that India's DPDP Act adopted some GDPR-inspired principles but followed a more flexible and government-oriented approach.

Researchers have also focused on the challenges faced by FinTech firms under these regulations. Arner, Barberis, and Buckley (2016) explained that FinTech companies require strong data governance because their operations depend on continuous data processing. Goodman and Flaxman (2017) highlighted concerns regarding AI-driven decision-making and the difficulty of explaining automated credit scoring systems under GDPR rules. Recent studies on India's DPDP Act by Parsheera (2023) and Joshi & Kaul (2023) further point out issues related to data localisation, regulatory uncertainty, and cross-border data transfers.

Overall, the literature shows that while both GDPR and the DPDP Act aim to protect personal data and build consumer trust, significant differences remain in their enforcement, transparency requirements, and regulatory philosophy. Scholars also identify continuing challenges related to consent management, AI accountability, data localisation, and balancing innovation with privacy protection in the evolving FinTech ecosystem.

3. RESEARCH OBJECTIVES

This study is guided by the following three research objectives:

1. To compare the GDPR and India's DPDP Act in terms of scope, consent, user rights, data transfer, enforcement, and their impact on FinTech companies.
2. To examine the compliance challenges faced by FinTech firms operating in both India and the European Union, especially in areas such as digital lending, AI-based credit scoring, open banking, and cross-border payments.
3. To suggest policy recommendations and a practical compliance framework that can help FinTech firms effectively comply with both data protection laws.

4. RESEARCH METHODOLOGY

4.1 Research Design

This study employs a doctrinal and comparative legal research design, supplemented by policy analysis and empirical evidence from regulatory enforcement records and industry impact assessments. The comparative method is well-established in legal research for identifying structural similarities and differences between legal systems and is particularly suited to the objective of analysing two distinct legislative frameworks within a common thematic domain — data privacy in FinTech.

4.2 Data Sources

The study draws on the following categories of secondary data and primary legal sources:

- Primary legal texts: The full text of the EU General Data Protection Regulation (Regulation (EU) 2016/679), the Digital Personal Data Protection Act, 2023 (India), and associated delegated regulations, recitals, and official guidance from the European Data Protection Board (EDPB) and India's Ministry of Electronics and Information Technology (MeitY).
- Regulatory enforcement data: GDPR enforcement tracker (enforcementtracker.com), European Data Protection Board annual reports (2018–2024), and MeitY notifications and press releases regarding DPDP Act implementation.
- Academic literature: Peer-reviewed articles from journals including the International Data Privacy Law, Computer Law and Security Review, the Journal of Financial Regulation, and the European Business Law Review.
- Industry reports: IAPP Global Privacy Benchmarking Reports (2020–2024), World Economic Forum FinTech and Data reports, Financial Stability Board cross-border data assessments, and PwC/Deloitte GDPR compliance surveys.
- Judicial and quasi-judicial decisions: European Court of Justice rulings on data protection

(including Schrems I and Schrems II), and relevant Indian Supreme Court and High Court decisions on privacy and data governance.

4.4 Limitations

The principal limitation of this study is the DPDP Act's incompleteness as of mid-2024: the detailed rules to be notified by the central government — covering inter alia the list of trusted countries for data transfer, the composition and procedures of the Data Protection Board, and sector-specific guidance — had not been published, necessitating reliance on the Act's text and available draft rule consultations. Additionally, GDPR enforcement outcomes vary across member states, making generalisation complex.

5.DATA ANALYSIS AND RESULTS

5.1 Scope and Territorial Application

The GDPR applies to the processing of personal data of individuals located in the EU, regardless of whether the processing takes place in the EU or elsewhere — a market-based extraterritorial principle with profound global implications. Any FinTech entity outside the EU that offers services to EU residents or monitors their behaviour is subject to GDPR, without any minimum transaction threshold. This has compelled Indian FinTech firms with EU users — including payments processors, digital remittance platforms, and cross-border lending apps — to appoint EU representatives and implement GDPR-compliant data governance systems.

The DPDP Act applies to the processing of digital personal data within India, and to processing outside India if it involves offering goods or services to individuals in India. Like the GDPR, it adopts a broad extraterritorial principle. However, unlike the GDPR's immediate applicability across all member states, the DPDP Act's provisions will take effect on a phased basis as rules are notified — introducing transition uncertainty for FinTech compliance planning.

5.2 Definition of Personal Data and Sensitive Data

The GDPR defines personal data broadly as any information relating to an identified or identifiable natural person. It creates a special category of 'sensitive personal data' covering health, biometric, genetic, racial, religious, and political data, subject to heightened processing restrictions. Financial data — such as transaction histories, credit scores, and bank account details — while not explicitly listed as sensitive, is treated as sensitive in practice by data protection authorities due to the severity of harms arising from its misuse.

The DPDP Act defines personal data as data about an individual who is identifiable from or in relation to such data. Notably, the DPDP Act does not create a separate category of sensitive personal data — a significant departure from India's earlier draft bills and from the GDPR. Instead, it empowers the central government to notify certain categories of data as subject to additional obligations, leaving the sensitive data framework incomplete pending rule notification. For FinTech firms processing financial, health-linked, and biometric data (common in digital KYC and lending), this ambiguity creates compliance risk.

5.3 Legal Basis for Processing and Consent Framework

The GDPR provides six legal bases for data processing: consent, contract, legal obligation, vital interests, public task, and legitimate interests. FinTech firms most commonly rely on consent and contract as their primary legal bases, with legitimate interests used for fraud prevention and security. GDPR consent must be freely given, specific, informed, and unambiguous — a high bar that invalidates pre-ticked boxes, bundled consent, and consent obtained as a condition of service. The GDPR's requirement for granular, purpose-specific consent has necessitated significant redesigns of FinTech onboarding flows, particularly for data-intensive services like credit scoring and behavioural analytics.

The DPDP Act establishes consent as the primary legal basis for processing, but also recognises 'legitimate uses' that do not require consent — including processing for the performance of a contract, compliance with law, medical emergencies, employment purposes, and functions of the State. For FinTech, the legitimate use carve-outs are significant: processing for loan disbursement, KYC compliance, and regulatory reporting can proceed without consent. The DPDP Act requires consent to be 'free, specific, informed, unconditional and unambiguous'

— closely mirroring the GDPR standard — and mandates the appointment of a Consent Manager for managing consent in complex data ecosystems.

5.4 Data Principal / Data Subject Rights

The GDPR provides a comprehensive suite of data subject rights: the right to access, rectification, erasure (right to be forgotten), restriction of processing, data portability, objection, and rights related to automated decision-making including profiling. The right to explanation under Article 22 — requiring that data subjects receive meaningful information about the logic of automated decisions significantly affecting them — is particularly consequential for FinTech algorithmic credit scoring, insurance pricing, and fraud detection systems.

The DPDP Act provides rights of access to information, correction and erasure, grievance redressal, and the right to nominate a representative to exercise rights on death or incapacity. Notably absent from the DPDP Act are the GDPR's right to data portability, right to restriction of processing, and — critically for FinTech — any right to explanation for automated decisions. This absence is significant: India's rapidly expanding algorithmic lending sector operates without a statutory obligation to explain adverse credit decisions to data principals, in contrast to the GDPR's Article 22 framework.

5.5 Cross-Border Data Transfer Mechanisms

The GDPR restricts transfers of personal data to third countries unless an adequacy decision is in place, or appropriate safeguards are implemented (Standard Contractual Clauses, Binding Corporate Rules, or approved codes of conduct). The Schrems II ruling of the Court of Justice of the European Union (2020) invalidated the EU-US Privacy Shield and tightened requirements for SCCs, requiring Transfer Impact Assessments (TIAs) for each cross-border data flow. India does not currently hold an EU adequacy decision, meaning that FinTech data flows from the EU to India require SCCs or equivalent safeguards — adding compliance complexity for cross-border FinTech operations.

The DPDP Act delegates the specification of trusted countries for outbound data transfers to the central government, which will maintain a 'whitelist' of permitted jurisdictions. This contrasts with the GDPR's 'blacklist plus safeguards' approach and creates asymmetric compliance obligations: Indian FinTech firms transferring data to the EU must comply with GDPR import requirements, while EU firms transferring data to India must await the Indian government's whitelist notification. Data localisation requirements — mandatory for certain sensitive categories of data — remain a point of regulatory tension between India's sovereign data governance philosophy and the GDPR's data portability and free flow commitments.

5.6 Enforcement Mechanisms and Penalties

The GDPR's enforcement architecture is among the most potent in global regulatory history. Penalties reach up to EUR 20 million or four percent of global annual turnover — whichever is higher — for the most serious violations. As of 2024, total GDPR fines across all sectors exceeded EUR 4.5 billion, with financial services and FinTech firms prominently represented. The DPC Ireland's EUR 1.2 billion fine against Meta (2023) for unlawful data transfers set a new precedent, signalling the GDPR's continued escalation of enforcement intensity.

India's DPDP Act establishes a Data Protection Board (DPB) as its enforcement authority, with penalty powers of up to INR 250 crore (approximately EUR 28 million) for significant breaches and INR 10,000 crore (approximately EUR 1.1 billion) for the most serious violations. While structurally significant, the DPB had not been constituted as of mid-2024, and no enforcement actions had been taken. Scholars including Parsheera (2023) have questioned the Board's independence, given its members' appointment and removal powers vested entirely in the central government — a structural concern absent from the GDPR's independently constituted supervisory authorities.

6. RESULTS AND DISCUSSION

6.1 Convergence: Shared Principles, Different Architectures

The GDPR and DPDP Act share a common philosophical foundation in the recognition of personal data protection as a fundamental right, the primacy of consent, and the principles of purpose limitation and data minimisation. For FinTech firms

operating across both jurisdictions, this convergence means that a strong data governance baseline — robust consent mechanisms, clear privacy notices, data retention limits, and breach notification protocols — is foundational to compliance with both frameworks. Firms that invest in GDPR-grade compliance infrastructure are well-positioned to meet DPDP Act obligations as rules are notified, since the GDPR represents the more demanding standard on most dimensions.

6.2 Divergence: Rights, Automation, and State Power

The most consequential divergences for FinTech are threefold. First, the DPDP Act's absence of a right to data portability undermines India's open banking vision: without a statutory right for data principals to move their financial data between institutions, the competitive benefits of account aggregation frameworks such as the Account Aggregator (AA) ecosystem rely on contractual and regulatory frameworks rather than statutory rights — a weaker foundation. Second, the absence of any right to explanation for automated decisions leaves Indian consumers of algorithmic credit, insurance, and investment products without statutory recourse against black-box decision-making. Third, the DPDP Act's broad government exemptions — permitting state entities to process data without consent for reasons of national security, public order, and sovereignty — create a two-tier privacy regime that the GDPR's more limited government exemptions do not.

6.3 Cross-Border Compliance: The Dual Regime Challenge

FinTech firms with operations in both India and the EU face a dual compliance burden that is greater than the sum of its parts. GDPR's Transfer Impact Assessment requirements for India-bound data flows impose legal, technical, and operational costs. Conversely, EU-bound data flows from India must satisfy SCCs or equivalent safeguards under GDPR, while simultaneously complying with whatever outbound transfer restrictions the DPDP Act's whitelist mechanism establishes. Until an EU-India adequacy arrangement is negotiated — a process that may take years and that requires India's data protection framework to satisfy the European Commission's adequacy criteria — cross-border FinTech operations will navigate a fragmented and uncertain regulatory landscape.

6.4 FinTech-Specific Compliance Priorities

For FinTech firms, four compliance areas demand priority attention under both frameworks. First, KYC and identity verification processes involve the processing of sensitive biometric and financial data; both GDPR and DPDP Act impose heightened obligations, though the GDPR's specific sensitive data category creates clearer compliance parameters. Second, algorithmic credit scoring requires GDPR-compliant automated decision-making safeguards that the DPDP Act does not yet mandate — creating an asymmetric compliance standard for firms operating in both markets. Third, data breach notification timelines diverge: GDPR mandates notification to supervisory authorities within 72 hours, while the DPDP Act requires notification 'as soon as possible' — a vague standard pending rule clarification. Fourth, consent management technology — Consent Management Platforms (CMPs) — must be configured differently for GDPR (opt-in, granular, withdrawable without detriment) and DPDP Act (similar in principle, but with different exceptions and the novel Consent Manager role).

7. CONCLUSION

This study shows that both the GDPR and India's DPDP Act aim to protect personal data, but they differ significantly in their approach and enforcement. The GDPR provides stronger user rights, stricter enforcement, and better safeguards for automated decision-making, making it a more comprehensive framework for FinTech regulation. In comparison, India's DPDP Act is an important step toward data protection but still lacks certain features such as data portability rights and clear protections against algorithmic bias.

For FinTech companies operating across India and Europe, complying with both frameworks is essential for maintaining trust and ensuring smooth cross-border operations. The study suggests that India should strengthen its rules on AI-driven decisions and improve regulatory clarity to align more closely with global standards. Overall, effective data privacy governance is becoming increasingly important for

building consumer confidence and supporting the sustainable growth of the digital financial ecosystem.

REFERENCES

1. Albrecht, J. P. (2016). How the GDPR will change the world. European Data Protection Law Review, 2(3), 287–289.
2. Arner, D. W., Barberis, J., & Buckley, R. P. (2016). FinTech, RegTech, and the reconceptualization of financial regulation. Northwestern Journal of International Law & Business, 37(3), 371–413.
3. Bhatia, G., & Kak, A. (2020). The Personal Data Protection Bill, 2019: A comparative analysis. IT for Change Working Paper. Bengaluru: IT for Change.
4. Chander, A., & Lê, U. P. (2015). Data nationalism. Emory Law Journal, 64(3), 677–739.
5. Cranston, R. (2018). GDPR compliance costs for FinTech startups: An empirical assessment. Journal of Financial Regulation, 4(2), 211–234.
6. European Data Protection Board (EDPB). (2024). Annual report 2023. Brussels: EDPB.
7. Financial Stability Board (FSB). (2019). FinTech and market structure in financial services. Basel: FSB.
8. Goodman, B., & Flaxman, S. (2017). European Union regulations on algorithmic decision-making and a 'right to explanation.' AI Magazine, 38(3), 50–57.
9. Greenleaf, G. (2022). India's DPDP Act 2023 in global context: A complex hybrid. Privacy Laws & Business International Report, 185, 1–7.
10. International Association of Privacy Professionals (IAPP). (2020). GDPR three years later: Compliance benchmarking survey. Portsmouth, NH: IAPP.
11. Joshi, P., & Kaul, A. (2023). Data localisation under India's DPDP Act: Implications for cross-border FinTech. National Law School of India Review, 35(1), 45–68.
12. Kuner, C., Svantesson, D. J. B., Cate, F. H., Lynskey, O., & Millard, C. (2020). GDPR: Two years on. International Data Privacy Law, 10(2), 83–85.
13. Parsheera, S. (2023). India's Digital Personal Data Protection Act 2023: An analysis. NIPFP Working Paper Series No. 402. New Delhi: National Institute of Public Finance and Policy.
14. Solove, D. J. (2006). A taxonomy of privacy. University of Pennsylvania Law Review, 154(3), 477–560.
15. Supreme Court of India. (2017). Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
16. Voigt, P., & von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR): A practical guide. Cham: Springer.
17. Wachter, S., Mittelstadt, B., & Russell, C. (2017). Counterfactual explanations without opening the black box: Automated decisions and the GDPR. Harvard Journal of Law & Technology, 31(2), 841–887.
18. Westin, A. F. (1967). Privacy and freedom. New York: Atheneum.
19. World Economic Forum (WEF). (2020). Data free flow with trust (DFFT): Paths towards free and trusted data flows. Geneva: WEF.
20. Zetzsche, D. A., Buckley, R. P., Arner, D. W., & Barberis, J. N. (2017). From FinTech to TechFin: The regulatory challenges of data-driven finance. New York University Journal of Law and Business, 14(2), 393–446.