DIGITAL TRANSFORMATION AND DATA PROTECTION IN INDIA: A COMPARATIVE STUDY WITH THE EU GDPR

Hemanth M V, LL.M., (Corporate and Commercial Law), School of Law, Christ (Deemed to be University), Bangalore, India

ABSTRACT

The purpose of this paper is to critically examine the evolving dynamics of digital transformation and data protection in India, with an in depth comparative analysis of India's recently enacted Digital Personal Data Protection (DPDP) Act, 2023, along with the European Union's General Data Protection Regulation (GDPR). As India experiences unprecedented growth in digital adoption across government services, financial technology, and the private sector, the volume and sensitivity of personal data processed have surged correspondingly. This transformation necessitates robust legal frameworks to protect individual privacy, regulate data fiduciary obligations, and establish effective enforcement regimes. While the GDPR serves as the world's leading model in comprehensive data protection, ensuring strong individual rights, explicit consent mechanisms, transparent cross-border transfer rules, and independent enforcement authorities, India's data protection framework is still nascent, marked by significant regulatory, legal, and operational gaps. The DPDP Act, 2023 introduces important reforms, including consent mandates, data principal rights, cross-border data transfer controls, and the establishment of a Data Protection Board. However, the Act includes broad government exemptions, centralized enforcement with potential executive override, and limited explicit protections for sensitive or automated decision-making data highlighting critical gaps compared to the GDPR. This paper investigates the nuanced legal provisions and practical challenges in both frameworks, focusing on consent requirements, data subject rights, enforcement mechanisms, cross-border data flows, and the impact of digital transformation on privacy and cybersecurity. It also addresses digital inclusion issues and challenges posed by evolving technologies like artificial intelligence. Findings reveal that while India's DPDP Act represents a significant stride toward data protection, enhanced legal clarity, decentralized and independent enforcement, inclusive mechanisms, and alignment with international standards are essential for a resilient data governance ecosystem. The study underscores the imperative for continuous reforms, increased digital literacy, and cross border cooperation to foster trust in India's expanding digital economy.

Keywords: Digital Personal Data Protection, GDPR, Data Privacy, Digital Transformation, Cross border Data Transfers.

Introduction

In the current era of rapid digitalization, personal data has become one of the most valuable assets driving economic growth, social interactions, and governance worldwide. India, with its vast and growing digital economy, has witnessed an unprecedented surge in data generation through digital platforms, e-governance initiatives, online financial services, and widespread smartphone penetration. As digital technologies become deeply embedded in everyday life, the protection of personal data emerges as a paramount concern, reflecting broader issues around privacy, autonomy, and national security. India's journey towards comprehensive data protection has been a gradual evolution from the Information Technology Act, 2000 and the corresponding privacy rules that primarily addressed limited aspects of sensitive data protection. These initial frameworks were insufficient to address complex challenges posed by big data analytics, cross-border data flows, and algorithm-driven automated decision-making. The recognition of the right to privacy as a fundamental right by the Supreme Court of India in 2017 set the stage for deliberate legislative reforms, leading to the enactment of the Digital Personal Data Protection (DPDP) Act, 2023. This statute represents a landmark in India's legal architecture, articulating a structured approach to data fiduciary obligations, consent management, data principal rights, grievance redressal mechanisms, and regulatory oversight through the Data Protection Board.

On the international stage, the European Union's General Data Protection Regulation (GDPR), enforced since 2018, remains the gold standard in privacy and data protection law. It introduced a comprehensive, enforceable, and uniform legal framework across EU member states, emphasizing individual data rights, clear obligations on data controllers and processors, stringent consent mechanisms, and robust enforcement powers for regulatory authorities. The GDPR is widely regarded as a model for countries globally seeking to align their data protection frameworks with international best practices.

This paper seeks to provide a detailed comparative study between India's DPDP Act and the EU GDPR, focusing on four core areas: individual rights afforded under each regime, obligations imposed on data fiduciaries, enforcement mechanisms, and provisions governing cross-border data transfers. The comparison helps reveal India's progress, limitations, and areas requiring reform for harmonization with global standards. Furthermore, the research explores the impact of India's digital transformation on privacy rights and data protection, highlighting

critical challenges such as cybersecurity threats, digital literacy gaps, and the inclusivity concerns of marginalized populations. It underscores the intersection of technological advancements with regulatory evolution and the vital role effective lawmaking plays in balancing innovation with privacy[1].

By drawing parallels and contrasts between India and the EU's models, this paper aims to contribute to the discourse on responsible data governance in the digital age and provide insights useful to policymakers, industry stakeholders, and civil society. The ultimate goal is to delineate pathways through which India can strengthen its data protection ecosystem, ensuring robust privacy safeguards while supporting its burgeoning digital economy.

The background of this study lies in the growing significance of personal data in India's digital economy and the global demands for robust privacy protections. Historically, India's regulatory approach relied on the Information Technology Act, 2000 and its amendments, which offered only fragmented safeguards for sensitive personal data and left critical gaps in comprehensive data protection. The exponential rise of digital platforms, cross-border data flows, and big data analytics exposed these legal deficiencies, placing India behind global standards like the European Union's GDPR. The GDPR, introduced in 2018, established a uniformly enforceable legal regime emphasizing consent, individual rights, and accountability for data processors across member states. By contrast, India's journey to the Digital Personal Data Protection (DPDP) Act, 2023 reflects years of legislative debate, demands for stronger legal clarity, and an increasing need to align domestic rules with international expectations to protect privacy, support global outsourcing, and foster confidence in India's digital transformation. This context provides the impetus for a comparative study focused on identifying regulatory gaps, operational challenges, and actionable pathways for harmonizing India's data protection framework with the best global practices[2].

India's digital transformation has surpassed the establishment of a robust data protection framework, as seen with the DPDP Act, 2023, which still faces significant gaps in enforceability, government exemptions, and individual rights protection. Compared to the GDPR, India's laws lack independent oversight, clear consent management, and transparent

[1] Sri Savithri Subbiah and A.Shanmuga Priyanga, *A Comparative Study on GDPR and DPDP, Act*, https://ijrpr.com/ ISSN 2582-7421

[2] Hemalatha G and Saikrupaa K, *Comparative Analysis on GDPR and Digital Personal Data Protection Act, 2023*, IJCRT.org, https://www.ijcrt.org/ Volume 11, Issue 12 December 2023 | ISSN: 2320-2882

cross-border transfer provisions. These shortcomings not only undermine privacy and public trust but also create operational uncertainties for businesses and impede alignment with global norms. The challenge remains to strengthen regulatory mechanisms and ensure inclusive, effective data protection for all citizens in an evolving digital landscape.

Research Questions

1. How do the provisions and principles of India's DPDP Act compare with the EU's GDPR regarding individual rights, data fiduciary obligations, and enforcement mechanisms?

2. What are the key similarities and differences in consent, cross-border data transfer, and government powers between India's DPDP Act and EU's GDPR?

3. How does digital transformation in India impact data privacy, and what challenges persist especially relating to cybersecurity and digital inclusion?

4. To what extent do current Indian regulations safeguard personal data and promote responsible data handling compared to the EU framework?

Research Objectives

1. To examine and compare the provisions of India's DPDP Act with the EU's GDPR, focusing on rights, obligations, and enforcement.

2. To identify similarities and differences in key areas such as consent, cross-border transfers, and government powers.

3. To assess the impact of digital transformation in India on privacy, with special reference to emerging challenges.

4. To evaluate the adequacy of Indian regulation in ensuring data protection and responsible handling, using the GDPR as a benchmark.

Research Methodology

This research adopts a qualitative, doctrinal methodology, focusing on comparative legal

analysis. The study is based on a review of statutes, judicial decisions, policy documents, and secondary academic literature relating to the DPDP Act and GDPR. Comparative insights are drawn from primary legislation, regulatory amendments, landmark case law, and scholarly articles to critically evaluate similarities, differences, challenges, and prospects. The gaps identified guide recommendations for regulatory evolution in India.

Literature Review

The literature review on Digital Transformation and Data Protection in India: A Comparative Study with the EU GDPR compiles insights from 10 sources spanning 2011 to 2024, predominantly highlighting India's historical deficiencies in comprehensive personal data protection prior to recent developments. Early works (Wankhede 2016, Duraiswami 2017, Singh 2011, Tyagi 2013) emphasize the inadequacy of the IT Act 2000 and its amendments/rules, which offered limited, narrow safeguards for sensitive data, lacked enforceability, relied on self-regulation or contracts, and failed to define key terms or impose broad obligations, creating significant gaps compared to the EU's evolving framework from the 1995 Data Protection Directive to the more robust, directly applicable GDPR (2016/2018, as discussed in Chase 2019, Keller 2017, Irani 2020). These studies repeatedly identify the absence of dedicated legislation, enforcement mechanisms, adequacy for cross-border transfers (labeling India an "insecure third country"), and balanced approaches to privacy versus business needs, with calls for holistic laws to boost competitiveness in outsourcing/IT sectors. Later contributions (Kulhari on blockchain-GDPR synergies, Sachin 2019/2024 on the DPDP Act's consent mechanisms and corporate impacts, Sinha 2024 on harmonization challenges across EU/US/India) reflect progress with India's Digital Personal Data Protection Act 2023 (DPDPA/DPDP Act), noting its revolutionary aspects like consent managers, fiduciary obligations, and cross-border restrictions, yet persisting research gaps include implementation ambiguities (e.g., consent withdrawal, breach notifications, joint responsibilities), limited flexibility in sensitive sectors like healthcare, insufficient actionable strategies for global harmonization beyond descriptive comparisons, and challenges in balancing privacy with innovation, enforcement, cultural contexts, and interoperability, gaps that remain relevant even as the DPDP Act moves toward phased enforcement (with core provisions gradually effective from 2025-2027). Overall, the reviewed literature underscores a persistent theme, while India has advanced from fragmented, inadequate protections to a more structured regime inspired by but distinct from the GDPR, critical gaps endure in comprehensive enforcement, definitional

clarity, practical cross-jurisdictional alignment, and addressing nuanced risks like profiling, intermediary liability, and overreach, necessitating further empirical and policy oriented research for effective global convergence.

Overview of India's DPDP Act, 2023 and EU GDPR, 2018

India's Digital Personal Data Protection Act, 2023 (DPDP Act), assented on August 11, 2023, marks the culmination of a tortuous legislative process, supplanting the withdrawn Personal Data Protection Bill, 2019. Having 44 sections, it establishes a consent driven regime for "personal data" any data identifying an individual (Section 2(t)) excluding non personal or anonymized data. Unlike the GDPR's breadth, the DPDP focuses solely on digital personal data, processed by "data fiduciaries" (controllers, Section 2(h)) with obligations to ensure accuracy, security, and erasure upon request.

Consent is pivotal (Section 5) free, specific, informed, unconditional, and unambiguous, with verifiable notices in clear language. Children under 18 require parental consent (Section 9), addressing vulnerabilities in tech and gaming. Rights mirror GDPR basics access, correction, erasure (Sections 11-13) but omit portability and objection to profiling, limiting empowerment.

The Data Protection Board of India (DPBI), appointed by the central government (Section 18), oversees enforcement, investigating breaches and imposing penalties up to ₹250 crore (Section 28). Appeals lie to the Telecom Disputes Settlement and Appellate Tribunal (Section 29), with civil courts for residual matters. Notably, Section 17[3] grants broad exemptions for government processing in "national security" or "public order," sans safeguards, raising autonomy concerns.

Cross-border transfers are permitted absent government restrictions (Section 16), a liberalization from localization demands, but lacking adequacy mechanisms. Significant data fiduciaries those processing large volumes face added duties like appointing India based data protection officers (Section 10).

In India's digital context, the DPDP aligns with UPI's 10 billion monthly transactions (NPCI, 2023) and Aadhaar's 1.3 billion enrollments, mandating breach notifications within 72 hours (Section 8). However, rule making powers vest in the executive (Section 40), delaying implementation, draft rules expected in 2024. Critics, including the Internet Freedom

[3] Digital Personal Data Protection Act, No. 22 of 2023, Sec. 17 (India).

Foundation (2023), decry centralized control and weak AI protections, potentially undermining trust in a nation where 900 million internet users grapple with phishing and deepfakes.

Overview on EU GDPR

Enacted on April 27, 2016, and effective from May 25, 2018, the General Data Protection Regulation (GDPR) represents a paradigm shift in data governance, harmonizing 28 disparate national laws across the EU into a unified framework. Administered by independent Data Protection Authorities (DPAs) in each member state, coordinated via the European Data Protection Board (EDPB), the GDPR applies to any entity processing EU residents' data, regardless of location Article 3's extraterritorial scope has ensnared global giants like Google and Meta in fines exceeding €2.5 billion since inception (EDPB, 2023).

At its core, the GDPR prioritizes principles under Article 5: lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, and accountability. Processing requires a lawful basis (Article 6), with consent (Article 7) demanding granularity, unambiguity, and revocability far beyond implied approvals. Sensitive data (e.g., biometrics, health) under Article 9 necessitates explicit consent or other stringent grounds.

Enforcement is decentralized yet potent. DPAs investigate complaints, impose corrective measures, and levy fines, with judicial oversight ensuring proportionality. Cross-border transfers (Chapter V) mandate adequacy decisions, standard contractual clauses (SCCs), or binding corporate rules (BCRs), prohibiting flows to "third countries" without safeguards Schrems II (2020) invalidated the EU-US Privacy Shield, tightening scrutiny.

The GDPR's integration with digital transformation is evident in its AI provisions, indirectly regulating automated decision making (Article 22)[4] to prevent discrimination. Amid EU's Digital Decade targets 80% digital skills proficiency by 2030 it balances innovation with privacy, fostering trust that has boosted e-commerce to €800 billion annually (Eurostat, 2023). Yet, challenges persist, compliance costs for SMEs and jurisdictional overlaps strain resources.

Legal Framework Governing Data Protection in India's DPDP and EU GDPR

The evolution of data protection laws in India has been spurred by the exponential growth of

[4] Regulation 2016/679, art. 22, General Data Protection Regulation, 2016 O.J. (L 119) 1 (EU).

digital technologies, socio-economic digitization, and the proliferation of private and public data repositories. India's legal journey began with patchwork protections provided by the Information Technology Act, 2000, and the IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. However, these regulations lacked clarity, enforceability, and the granularity to address modern data privacy challenges, especially against the sophisticated legislative backdrop of the European Union.

The DPDP Act, 2023 marks the country's first comprehensive data protection statute, redefining rights, obligations, and enforcement mechanisms. Data principals, or individuals whose data is processed, are empowered with the rights to access, correct, erase, and receive notification regarding use, breach, and transfer of their personal data. Data fiduciaries are obligated to ensure lawful, fair, and transparent processing and are subject to penalties for violations.

The Act also establishes the Data Protection Board for adjudication and enforcement. In contrast, the GDPR is lauded for its exhaustive framework that transcends geographical boundaries. Its extraterritorial reach requires any organization worldwide to comply with its provisions if they process data of EU residents.

The GDPR meticulously details data subject rights, consent standards, processor/controller obligations, breach notifications, and even the right to human intervention in automated decisions. Enforcement is decentralized through national Data Protection Authorities, coordinated by the European Data Protection Board (EDPB). Penalties are among the harshest globally, with the ability to levy fines up to €20 million or 4% of global turnover.

The Digital Personal Data Protection (DPDP) Act, 2023 is India's first legislation dedicated exclusively to personal data protection. It lays out principles of fairness, consent, transparency, and redress, establishing data principal rights, data fiduciary obligations, rules for cross-border data transfers, and a structure for enforcement through the Data Protection Board of India. However, the DPDP Act retains critical exemptions for government actions, creates a centralized and arguably non-independent enforcement regime, and lacks granular provisions for sensitive data, children's data, or algorithmic transparency[5].

[5] Duraiswami, Dhiraj R. *"Privacy and Data Protection in India."* Journal of Law & Cyber Warfare 6, no. 1 (2017): 166–86. http://www.jstor.org/stable/26441284.

The European Union, conversely, has long been the world's gold standard for data protection. The General Data Protection Regulation (GDPR), enforced since 2018, is a sweeping, harmonized law covering all member states and any entity handling the data of EU residents, regardless of global location. The GDPR provides extensive data subject rights: access, correction, erasure ("right to be forgotten"), portability, objection, and restriction, supported by clear legal bases for processing. Independent and distributed Data Protection Authorities (DPAs) ensure rigorous compliance, backed by the European Data Protection Board's regulatory oversight[6].

Comparison between DPDP Act and GDPR

The Digital Personal Data Protection (DPDP) Act, 2023 signifies India's first landmark legislative attempt at a comprehensive data protection framework, aiming to regulate personal data management amid the country's rapid digital transformation. Modeled in part to align with global benchmarks like the European Union's General Data Protection Regulation (GDPR), the DPDP Act establishes fundamental principles such as transparency, consent, purpose limitation, and accountability for data fiduciaries. However, while both frameworks share common goals of protecting individual privacy and regulating data processors, substantive differences underscore divergent legal philosophies, governance structures, and contextual socioeconomic needs.

One of the pivotal distinctions lies in the scope and comprehensiveness of individual rights. The GDPR provides a broad spectrum of enforceable rights for data subjects, including the right of access, rectification, erasure (the "right to be forgotten"), data portability, and the right to object to processing. Its provisions also explicitly regulate automated decision-making and profiling, thereby safeguarding individuals from opaque algorithmic impacts. Conversely, the DPDP Act, while granting access, correction, and erasure rights, omits data portability and explicit objection mechanisms. It lacks clear regulatory provisions addressing algorithmic accountability, signaling an area wherein Indian legislation remains nascent relative to the GDPR, reflecting both legislative timing and differing policy priorities[7].

[6] Wankhede, Asang, *Data Protection in India and the EU: Insights in Recent Trends and Issues in the Protection of Personal Data* (January 1, 2016). European Data Protection Law Review (EDPL) 2016, Issue 1, 1-10, https://dx.doi.org/10.2139/ssrn.3899865

[7] Anita Yadav and Rabikant Pandey, *Data Privacy across Borders: A Comparative Analysis of European Union and Indian Protection* , https://heinonline.org

Consent, foundational to lawful data processing in both regimes, also shows nuanced divergence. GDPR mandates that consent be freely given, specific, informed, and unambiguous, with an emphasis on easy withdrawal at any time. The DPDP Act requires user consent but includes provisions permitting exceptions for "legitimate purposes" as defined by the government, which introduces greater legal ambiguity. This flexibility may aid business operations and public administration but risks diluting individual autonomy, a tradeoff reflective of India's balancing of rapid digital growth with privacy protections.

Cross-border data transfer mechanisms exemplify another significant difference. The GDPR tightly regulates transfers outside the EU, permitting them only where countries ensure "adequate" protection, or where controllers adopt EU-approved standard contractual clauses or binding corporate rules. India's DPDP Act currently governs cross-border transfers through government-issued notifications and permits reliance on adequacy-like determinations, but the legislative and operational framework remains less transparent and less predictable. This may hamper India's position as a global data processing hub, obligating Indian companies to navigate complex compliance and contractual requirements vis-à-vis overseas clients and regulators.

Recent Amendments to India and European Data Protection Laws

The DPDP Act, 2023, followed by the draft DPDP Rules 2025, brings India closer to global norms. Key new features include phased implementation for businesses, data breach notification duties, and more precise obligations on startups and SMEs. However, the rules retain ambiguity on cross-border transfer protocols and government-related exemptions, sparking debate about regulatory predictability.

The GDPR amendments of 2024 have enhanced enforcement efficiency for cross-border cases, increased fines for repeat offenses, introduced faster DPIA procedures, and responded to AI and algorithmic risks with transparency and human intervention mandates. These changes reflect the EU's approach to constantly evolving digital threats and regulatory effectiveness[8].

Applicability in Cross border Transactions

Cross-border data flows constitute a cornerstone of the global digital economy, enabling

[8] K. S. Sachin, *"Balancing Privacy: Unraveling India's Personal Data Protection Act and Its Impact on Corporate Realms"*, 4 LEGAL LOCK J. 82 (2024)

services like cloud computing, international outsourcing, e-commerce, and global communication. For countries like India, significant economic activities depend on processing personal data across geographical boundaries, especially in sectors like IT-BPO, fintech, and social platforms. This reality makes the regulation of cross-border transfers a critical component of any data protection framework's applicability and effectiveness.

Under the Indian Digital Personal Data Protection (DPDP) Act, 2023, cross-border transfers of personal data are subject to specific provisions but exhibit relative legislative discretion. The Act empowers the central government to issue notifications specifying conditions for the transfer of personal data outside India. Transfers can only occur under conditions deemed adequate or compliant with prescribed safeguards as notified. This delegation of authority to the government introduces flexibility but also uncertainty for businesses, given the lack of clear, uniform, and publicly accessible adequacy frameworks or standardized contractual clauses equivalent to the EU's mechanisms. The absence of a well-defined procedure for assessment and recognition of adequacy or binding corporate rules means Indian data fiduciaries face operational and legal challenges when dealing with international clients, impacting India's competitiveness as a global data processing hub. This ambiguity can increase compliance costs and risks, especially for small and medium enterprises struggling to interpret or manage complex international trade privacy obligations.[9]

In contrast, the EU General Data Protection Regulation (GDPR) establishes one of the most comprehensive and structured regimes regulating international data transfers[10]. The GDPR restricts personal data flow outside the European Economic Area (EEA) unless the recipient country or entity provides data protection "adequacy" comparable to EU standards. Adequacy decisions are made based on a thorough assessment of the third country's legal environment and enforcement practices. In the absence of adequacy, organizations must rely on legally binding instruments such as Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs), or explicit informed consent from data subjects. This layered approach combines legal certainty with flexibility and enforces clear accountability on data exporters and importers alike. GDPR's extraterritoriality applies these rules not only to EU-based companies but to any

[9] Vivek Kumar Tyagi, *Legal Offshoring Industry and Data Privacy: Global Perspectives (With Special Reference to India)* (2013)
https://www.jstor.org/stable/24701061
[10] Peter H Chase, *Perspectives on the General Data Protection Regulation Of the European Union (2019)*
http://www.jstor.com/stable/resrep21227

entity handling data of EU residents globally, reinforcing the breadth and influence of the regime.

India's regime currently lacks similar mechanisms. The DPDP Act's government driven, notification-based approach to cross-border transfers has yet to codify standardized clauses or rules for international adequacy notably delaying India's acquisition of an EU adequacy status essential to facilitate frictionless data exchange. Without an official adequacy decision or harmonized transfer frameworks, Indian firms must often navigate complex contractual assurances with stiff compliance burdens that may deter or limit digital trade and international partnerships. While Indian policymakers have expressed intent to enhance alignment with global standards in future rules, the current legal landscape reflects a transitional phase.

Cybersecurity: Digital Risk Management and Legislative Response

With the rise of cloud services, IoT, AI, and pervasive digital footprints, India faces escalating risks: cyberattacks, phishing, ransomware, breaches of public sector databases, and exposure of PII. The DPDP mandates "reasonable security practices," but detailed standards, prescribed audits, or sector-specific obligations are rare, especially for SMEs.The GDPR is more rigorous, requiring "privacy by design," DPIAs, mandatory breach notifications within 72 hours, and technical safeguards for all processors/controllers. European regulators proactively supervise, audit, and fine breaches, compelling corporations to build resilient infrastructure and train staff.

The GDPR is more rigorous, requiring "privacy by design," DPIAs, mandatory breach notifications within 72 hours, and technical safeguards for all processors/controllers. European regulators proactively supervise, audit, and fine breaches, compelling corporations to build resilient infrastructure and train staff[11].

India's cybersecurity landscape is challenged by a skills gap, inconsistent enforcement, lack of standardized breach notification, and technical illiteracy. Cooperative models with CERT-In, sectoral regulators, and community awareness initiatives are emerging but cover only a fraction of risks.

[11] Keller, Daphne, *The Right Tools: Europe's Intermediary Liability Laws and the EU 2016 General Data Protection Regulation* (March 22, 2017), http://dx.doi.org/10.2139/ssrn.2914684

Practical Implementation Gaps

1. The Data Protection Board's limited staff, regional absence, and centralized control constrain its effectiveness.

2. Regulatory attention is focused on large entities, risking neglect of smaller businesses and startups.

3. Lack of clarity in consent processes, withdrawal protocols, breach notifications, and complaint resolution undermine public trust.

4. Training, technical resources, and international harmonization are critically required.

These complexities showcase why a robust, rights-based, and technically capable regulatory ecosystem is essential for India's digital transformation. By examining contemporary legislation, enforcement reality, and comparative lessons from the GDPR, the research highlights both achievements and persistent gaps in India's approach to personal data protection. The analysis is vital for policymakers, business leaders, rights advocates, and academic observers committed to safe, inclusive, and globally harmonized digital futures[12].

Landmark Cases

European Union

1. ***Schrems II (Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, 2020)***

This landmark judgment by the Court of Justice of the European Union (CJEU) invalidated the EU-US Privacy Shield framework, a key mechanism allowing transatlantic data transfers. The court held that US surveillance laws do not provide adequate protection under EU standards, particularly failing in the right to effective judicial remedies. The decision underscored the GDPR's strict adequacy requirement for cross-border data transfers and emphasized the need for additional safeguards, such as Standard Contractual Clauses.

[12] Sharmin Godrej Indrani, *Application of General Data Protection Regulation on Indian Processor* (2020) https://www.scconline.com/blog/post/2020/05/12/application-of-general-data-protection-regulation-on-indian-processor/

Outcome: This ruling forced companies to reassess their international data transfer mechanisms, significantly impacting global data flow and compliance practices.

2. ***Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González (2014)***[13]

Although predating GDPR, this case laid the foundation for the "Right to be Forgotten," now enshrined in GDPR Article 17. The CJEU ruled that individuals have the right to request removal of personal data from internet search results when such data is outdated, irrelevant, or excessive. This case reinforced individual control over personal information, influencing GDPR's provisions on data erasure.

Landmark Cases under India's DPDP (or Predecessor Legal Framework)

1. ***Justice K.S. Puttaswamy v. Union of India (2017)***[14]

The Supreme Court of India declared the Right to Privacy as a fundamental right under Article 21 of the Constitution. This judgment laid the constitutional foundation motivating India's data protection legislation. It stressed the need for "informational privacy" and balanced individual rights against state interests, impacting subsequent policy making.

2. ***Aadhaar Data Breach Cases (2018-2023)***

Several petitions challenged the privacy and security of biometric data under the Aadhaar scheme, highlighting vulnerabilities in government data processing. Courts noted the lack of adequate legal safeguards and procedural transparency. These cases pressured legislative efforts toward comprehensive data protection laws.

3. ***Boat Data Breach Incident (2023)***

The data breach involving personal and payment information of millions of Indian customers of boat highlighted the insecurity in private sector data practices. While not adjudicated at the Supreme Court level, this case became a critical reference point showing the gaps in

[13] *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, **ECLI:EU:C:2014:317.**
[14] Justice K.S. Puttaswamy (Retd.) &Anr. v. Union of India & Ors, (2017) 10 SCC 1 (India).

enforcement under existing rules and the urgent need for the DPDP Act.

Conclusion and Suggestion

India's Digital Personal Data Protection Act, 2023, marks a pivotal advancement in safeguarding privacy amid the nation's explosive digital transformation, yet it reveals stark contrasts with the EU's GDPR, underscoring the need for deeper alignment with global benchmarks. While the DPDP Act introduces essential mechanisms such as consent mandates, data principal rights, and the Data Protection Board, its broad governmental exemptions, centralized enforcement susceptible to executive influence, and limited safeguards for sensitive data and automated decision making expose vulnerabilities. These gaps, when exposed against the GDPR's robust individual empowerment, independent oversight, and stringent cross-border transfer protocols, highlight how India's framework, though progressive, risks undermining public trust and operational efficacy in an era of AI-driven analytics, big data flows, and cybersecurity threats.

The surge in digital adoption spanning e-governance, fintech, and ubiquitous smartphone penetration amplifies these challenges, particularly for marginalized populations grappling with digital literacy deficits and exclusionary risks. By bridging these regulatory chasms, India can transform privacy from a mere legal obligation into a catalyst for inclusive growth, ensuring that technological progress empowers rather than erodes individual autonomy in the global digital landscape.