Data Privacy Governance Under India's DPDP Act, 2023 and the EU GDPR: A Comparative Study with Focus on Cross-Border Data Transfers

Declaration:

We hereby declare that this paper is our original work, has not been submitted elsewhere for publication, and is not under consideration with any other journal/platform.

Authors:

Shaily Agrawal (corresponding author)

Research Scholar (Law)

Jagran Lakecity University

Dr. Yash Tiwari

Associate Professor (Law)

Jagran Lakecity University

Abstract

The personal data has grown significantly with worldwide transmission due to the rapid expansion of digital ecosystems, making data privacy management an essential concern for companies operating across nations. The study conducts a comparative analysis of the Digital Personal Data

Protection (DPDP) Act, 2023, and the General Data Protection Regulation (GDPR) from an operational and administrative perspective. It focuses on the prerequisites for organizations to comply with the law, data processing rules, consent, and cross-border data management. Employing a comparative interpretative approach, the paper analyzes academic papers, legal frameworks, and regulatory specifications to identify convergences and divergences of the two regimes. The primary outcomes reveal that the DPDP Act focuses on accountability and consent-based processing, whereas the GDPR takes a broader and rights-based approach. For the cross-border data transfers, a thorough examination reveals that the GDPR uses standard clauses, including adequacy decisions and Standard Contractual Clauses (SCCs), while the DPDP Act works according to the blacklist model approved by government. In the end, the paper concludes that transparency regarding regulations and better connectivity procedures could streamline international data management, ensuring the privacy of data in digital activities across borders.

Keywords - Data privacy; GDPR; DPDP Act 2023; Cross-border data transfers; Consent management; Privacy compliance.

1. Introduction

1.1 Background and Rationale

Communication, commerce, innovation, and governance, all sectors of society have been affected by the digital ecosystem globally. The technological advancements have rendered it feasible for individuals and companies to share information across borders in novel and unseen ways. Data has become an important economic resource and also a component of modern life's infrastructure (UNCTAD, 2021). The digital economy depends on cross-border data flows, which enable digital services such as cloud computing, digital payments, social media, health information systems, and artificial intelligence (AI) apps (OECD, 2022).

As the value of data increases, the exploitation, misuse, and unauthorized access of data increase as well. Digital surveillance, cyberattacks, and breaches of privacy have raised concerns regarding personal data management (Solove, 2008). Therefore, countries

worldwide are developing guidelines to protect personal data while promoting economic growth and technological innovation (Greenleaf, 2023).

The General Data Protection Regulation (GDPR) is regarded as the most significant and comprehensive privacy law globally (GDPR, 2016). It sets guidelines on data privacy, cross-border transfers, and corporate accountability (Voigt, & Von dem Bussche, 2017). Under GDPR rules for cross-border data transfer is quite strict as privacy is considered a fundamental right (GDPR, 2016, Recital 1). So the standards for data transfer under GDPR, the Adequacy Mechanisms, Standard Contractual Clauses (SCCs), and Binding Corporate Rules (BCRs), ensure data transmitted outside the European Union (EU) is given the same level of protection as within the EU (European Commission, 2023).

The Digital Personal Data Protection Act, 2023 (DPDP Act) of India exhibits a unique legislative framework originating from the Global South (DPDP Act, 2023). India is undergoing rapid expansion in its digital market, with predictions demonstrating a digital economy valued at USD 2 trillion by 2030. This growth is due to vast digital infrastructure and expanding e-commerce platforms (Press Information Bureau, 2024). The DPDP Act completed the comprehensive privacy reform, which began with Justice K.S. Puttaswamy v. Union of India (*Justice K.S. Puttaswamy (Retd.) v. Union of India*, 2017). Unlike the GDPR, the DPDP Act permits cross-border data flows to most jurisdictions except those specifically banned by the central government (DPDP Act, 2023, s. 16). This shows a strategic policy change to encourage digital trade and commerce between nations.

The cross-border data transfer regulations regarding data privacy are different in various jurisdictions which leads to the conflict between individual rights, state sovereignty, and commercial interests. Protection of personal data must be balanced with development of economic potential of various countries. Although strict rules can promote trust and accountability, they could additionally slow down trade and creativity. On the other hand, flexible rules could assist in economic growth, but they make people vulnerable to privacy risks (Kuner, 2013).

The comparison of GDPR and the DPDP Act reveals differences. The GDPR has high standards for transmitting data with risk assessments and procedural safeguards (Voigt, & Von dem Bussche, 2017). In contrast, the DPDP Act has fewer transfer conditions, facilitating transparency, but has gaps in supervision, protections, and individual compliance (Kumar, 2025).

Data privacy has a vast scholarly literature, but little has been written about cross-border data transfers from a technical and administrative perspective. The traditional method of legal analogies focuses on interpretation, rights, and compliance requirements. They do not consider how institutions or organizations operate, technological dependencies, or foreign policies.

This research gap is fulfilled by this article. In this paper, the cross-border data transfer rules of both frameworks are studied based on governance of rights, risks, and the state. Each system is assessed for privacy, risk management, transfer structure, sovereignty, and global digital integration. The effects of corporate conformity, digital trade, and future harmonization are also examined.

1.2 Research Objectives

The primary objectives of this study are: -

1. To compare the fundamental concepts and enforcement goals of the GDPR and the DPDP Act.
2. To examine methods of getting consent and lawful processing in both frameworks.
3. To evaluate corporate accountability, including duties of data fiduciaries.
4. To analyze data subject rights and remedies, identifying gaps in the two frameworks.
5. To assess cross-border data transmission ways and compliance problems.
6. To suggest policies to make global data regulation interoperable and consistent.

2. Methodology

This research employs a comparative qualitative research method to examine data privacy regulations under the DPDP Act and GDPR. Comparative analysis is utilized in regulatory and

administrative research to compare legal and policy systems and their functional consequences (Caron et al., 2015; Zweigert & Kötz, 1998). Data governance is globally distributed, and global data flows are becoming more intricate, so qualitative interpretive methods can identify structural patterns and regulatory outcomes that quantitative methods cannot measure (Bryman, 2016).

2.1 Research Design

The study incorporates documentary analysis and analyzes regulatory documents, scholarly literature, policy reports, and commentaries. The comprehensive review of legal and policy material enables a deeper understanding of regulations, data-processing duties, and cross-border data transfer systems (Bowen, 2009). The approach incorporates legal literature, information systems study, and regulatory governance studies.

2.2 Data Sources

There are following types of data utilized in the study: -

1. Primary Laws - The GDPR and the DPDP Act
2. Academic Writing -Refereed books and papers on data flows, privacy, consent, and accountability (Greenleaf, 2023; Kuner, 2013).
3. Reports and Regulatory Guidelines - EU Data Protection Authorities (DPAs) guidelines, EDPB opinions, and explanatory notes from the Indian government.

2.3 Comparative Framework

A functional comparative method is employed in the study, which focuses on the objective and impact of provisions rather than written form (Zweigert & Kötz, 1998). The study looked at five main areas –

- fundamental principles,
- consent and processing conditions,
- data controller duties,
- data subjects' rights, and
- means for transferring data across borders (Kuner, 2013; Tufekci, 2015).

2.4 Analytical Method

Requirements of management, compliance and transfer were discovered by categorizing documents using an interpretive method. Important procedures included finding common trends, charting similar or different rules, examining corporate implications, and analyzing privacy consistency or disintegration. Thematic analysis allows ethical content comparison and regulatory details (Braun & Clarke, 2006).

2.5 Scope and Limitations

The management of personal data according to the two regulations is mainly studied in this study. The sectoral rules, cyber laws, and AI frameworks that are relevant are included. The system has some flaws, but gives an effective way to examine regulatory systems and data flows across borders.

3. Literature Review

The literature is quite vast including the following points: -

3.1 Evolution of Global Data Protection Laws

The rise of information-based economies has raised global concerns about surveillance, algorithmic processing, and cross-border data transfers, expediting data privacy governance across jurisdictions. With the increase in the digital data flows, it is witnessed that the data protection systems have shifted from sectoral to holistic models (Greenleaf, 2023). According to various theories, privacy laws have two important jobs: -

a. safeguarding the rights of individuals and
b. establishing trust in digital systems (Solove, 2008).

Digital services like cloud-based computing and international trade require cross-border data, and to control data transmitted to other countries, legal protections are put in place by the state (U.S. Congress, Congressional Research Service, 2022). These events demonstrate the conflict between economic integration and autonomous data management.

3.2 GDPR – A Global Benchmark

The rights-centric foundation of the GDPR, based on the EU Charter of Fundamental Rights, has been described by academic literature as its unique feature (Voss, 2022). Lawfulness, transparency, purpose limitation, and accountability are among the strict principles of the regulation, creating a gold standard, as opined by some scholars (Voigt, & Von dem Bussche, 2017). Businesses outside the EU handling personal data of EU residents are subject to its regulations because of its extraterritorial scope (Tufekci, 2015).

3.3 India's Data Privacy Law - the DPDP Act, 2023

The Supreme Court's recognition of privacy as a fundamental right, the growth of data-based services, and the country's rapid digitization have helped pave India's path towards a comprehensive data protection regime. Privacy is essential to dignity and personal liberty was upheld in Justice K.S. Puttaswamy v. Union of India (2017), facilitating the enactment of a national data protection law (*Justice K.S. Puttaswamy (Retd.) v. Union of India*, 2017). Early drafts of India's data protection bill were based on the GDPR, but with subtle adjustments addressing economic and administrative issues (Lakra et al., 2025).

Under the DPDP Act, there is a balance between the user rights and corporate accountability (Latham & Watkins LLP, 2023). According to some scholars, the Act emphasizes consent-based processing, requirements for significant data fiduciaries, simplifying compliance compared to the GDPR (Latham & Watkins LLP, 2023). The Act differs from GDPR’s approach due to a lack of processing rules, centralized management, and dependence on government-approved transfer procedures (Nishith Desai Associates, 2023). An emerging governance-based approach is seen in corporate duties for notice, consent, security precautions, and breach notifications.

3.4 Comparative Cross-Border Data Transfers

Cross-border data transfer is one of the most disputed issues in global data management due to competing interests in privacy, trade, security, and digital sovereignty. According to scholars, multinational corporations experience compliance challenges due to the lack of uniformity in the global regulatory landscape (U.S. Congress, Congressional Research

Service, 2022). The data transfer methods under GDPR have been criticized for being difficult and non-adaptable in international situations (Voss, 2022).

The research on cross-border system under DPDP Act is limited, as it has been enacted two years back and just got implemented. While the whitelist method of India of cross-border data transfer is easy to implement, but also unpredictable due to administrative discretion (Latham & Watkins LLP, 2023). To help India participate in global electronic markets and reduce compliance complexities, comparative privacy specialists argue that interconnection with global frameworks is crucial (Latham & Watkins LLP, 2023).

3.5 GDPR and Indian Data Protection Laws

The comparative analysis of GDPR and India's past data protection drafts reveal basic distinctions of principles, and legal structure (*Justice K.S. Puttaswamy (Retd.) v. Union of India*, 2017; Lakra et al., 2025). However, because of its recent implementation, there are still few comparative studies, especially discussing the DPDP Act. The literature highlights the distinctions between the DPDP Act's approach based on governance and accountability and the GDPR's rights-based foundation (Nishith Desai Associates, 2023).

The literature on cross-border systems of the two frameworks is less. Both Voss (2022) and Greenleaf (2023) underline the need for more research to understand the emerging privacy regulations interact with existing structures like the GDPR. Researchers who study information systems also state that companies require unified compliance strategies for conducting their cross-border operations smoothly (Greenleaf, 2021).

3.6 Identified Research Gap

There is significant research on the GDPR and the DPDP Act separately, but there is a lack of comparative research focusing on: -

- methods trans-border Data Transfer;
- management structures for operational compliance;
- the implications for multinational organizations that need to comply with both laws, and

- variations in surveillance by regulators, consent setup, and accountability.

This study seeks to address the gaps identified by comparing the two regimes in an organized manner and considering the effects on data privacy laws around worldwide.

4. Results and Discussion

This study compares the two systems and examines their laws, duties, and ways of transferring data, shape global data control, and business compliance.

This section covers five main topics: -

- fundamental concepts,
- consent and legal processing,
- corporate accountability, rights for individuals, and
- cross-border transfer methods.

4.1 Foundational Principles and Regulatory Rights

A rights-based approach, the GDPR recognizes personal data protection as a fundamental right guaranteed by the European Union Charter (Voss, 2022; Charter of Fundamental Rights of the European Union, 2012). The principles of GDPR - lawfulness, fairness, transparency, purpose limitation, accuracy, storage limitation, integrity, and accountability regulate all data-processing operations and provide consistent regulations (Voigt, & Von dem Bussche, 2017). Also, these principles ensure that organizations' duties are clear and enforceable.

On the other hand, the DPDP Act is simple in structure with fewer well-written principles. Some of the GDPR's principles, like fairness, openness, and data minimization, are not expressly mentioned in this Act. However, it reiterates the importance of consent, purpose limitation, lawful processing, and security measures. A possible explanation for this omission is that the Act was designed to simplify compliance for businesses in India's rapidly expanding digital economy (Latham & Watkins LLP, 2023).

4.2 Consent and Lawful Processing

According to the GDPR, consent must be freely given, clear, specific, informed, and not ambiguous. Additional safeguards must be provided to secure sensitive personal data (GDPR, 2016, Arts. 4–7). The legal bases that provided by the GDPR include contractual necessity, legitimate interest, legal duty, and vital interests. This gives them operational flexibility (Greenleaf, 2023).

While the DPDP Act mainly relies on consent or deemed consent for processing, it has more exceptions for areas like jobs, medical conditions, and government duties (Nishith Desai Associates, 2023). Unlike the GDPR, the DPDP Act does not provide alternatives such as legitimate interest, restricting choices for private sector entities (Latham & Watkins LLP, 2023). To comply with both GDPR and DPDP, the multinational companies need to ensure sure that their consent procedures fulfil both laws.

4.3 Organizational Accountability and Governance Structures

The GDPR requires extensive accountability, such as Data Protection Impact Assessments (DPIAs), Data Protection Officers (DPOs), records of processing activities, and privacy-by-design standards (Voss, 2022). These standards of obligations give a compliance-based environment and clear operational standards.

As per the DPDP Act only Significant Data Fiduciaries (SDFs), chosen according to the volume of data they process and the associated risks, need to follow strict duties. Such duties are not mandatory for non-significant data fiduciaries to follow. The significant data fiduciaries need to hire data protection officers, do data protection impact assessments, and be audited on a regular basis. Consequently, the compliance formalities for smaller companies becomes easier to follow but international compliance for large corporations is adversely affected which work with company procedures across jurisdictions.

4.4 Rights of Data Subjects and Data Principals

The right to access, correction, erasure, restriction, portability, and objection are among the many rights provided to data subjects by the GDPR (Voigt, & Von dem Bussche, 2017).

These rights promote the rights-driven approach of GDPR and offer people greater control over their personal data.

The rights by the DPDP Act include access, correction, erasure, and grievance redressal, and it fails to address objections, restrictions, or portability (Latham & Watkins LLP, 2023). The right to erasure under this Act is wide in some circumstances, but it remains subject to government discretion. This may simplify GDPR compliance for Indian firms but cause interoperability issues for big firms.

4.5 Cross-Border Data Transfer Mechanisms

In today's digital age, cross-border data transfer is necessary to have digital activities at a global level. Adequacy decisions, Standard Contractual Clauses (SCCs), and Binding Corporate Rules (BCRs) are three mechanisms provided by the GDPR that guarantee data receives the same level of protection outside the European Union (Voss, 2022). Schrems II and other judgements have highlighted the multifaceted nature of operations and the need to conduct transfer impact assessments (*Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems v. Data Protection Commissioner (Case C-311/18) [Schrems II]*, 2020).

Under the DPDP Act, transfers are permitted only for countries that are not blacklisted by the central government and provide adequate protection (Latham & Watkins LLP, 2023). This approach is easy to follow, but the executive gets a lot of autonomy, which could make it tough for businesses in areas like global trade or cloud-based services (Latham & Watkins LLP, 2023). International enterprises deal with various laws and regulations, and they need to implement different security strategies for every region.

4.6 Overall Interoperability and Organizational Implications

Although both frameworks seek to protect privacy and promote accountability, the research shows that the GDPR takes a principle and rights-based approach, while the DPDP Act is more governance-oriented with a limited compliance strategy.

Major implications on multinational companies include: -

- Handling multiple legal bases for processing;
- setting up concurrent rights-management systems;
- aligning paperwork and accountability procedures; and
- addressing diverse cross-border transfer regimes

Thus, flexible data sharing procedures can help in ensuring that digital procedures around the world run smoothly (Greenleaf, 2023; Voss, 2022)

5. Policy Recommendations

This study highlights various policy issues and concerns for companies and regulators. The following suggestions may help improve data handling techniques: -

5.1 Recommendations for Regulators

a. **Synchronized Frameworks –** The governments of various jurisdictions must consider synchronizing the implementation of GDPR and the DPDP Act. Multinational enterprises can reduce conflict with bilateral agreements and local data transfer agreements (Greenleaf, 2023).

b. **Cross-border Transfer Mechanisms –** If regulators consider standards like the GDPR's adequacy decisions, Standard Contract Clauses, and Binding Corporate Rules, the cross-border transfer paths can be made simple more certain. To enhance digital trade globally, the system needs to be updated (Latham & Watkins LLP, 2023).

c. **Unambiguous Explanation of Rights and Obligations -** The guidelines for various sectors and things like risk assessments program details must be provided by the regulators. This can reduce gaps and help business operations function in an optimized manner (Lakra et al., 2025).

d. **Improving Supervision and Accountability –** For effective implementation of DPDP Act, the processes of GDPR can be followed. These processes include audit procedures, and risk assessments.

5.2 Recommendations for Industry

a. **Integrated Compliance Strategies –** Businesses with operations in the European Union and India are required to establish standardized compliance mechanisms that

may function collectively to handle issues involving data subjects' rights, consent management, lawful processing, grievance procedures, and paperwork requirements (Voss, 2022).

b. **Privacy-by-Design Implementations –** The principles of privacy-by-design and privacy-by-default can benefit the companies a lot to be in line with the GDPR and the DPDP Act.

c. Cross-Border Data Handling Protocols – To analyze third-country data privacy laws, conduct transfer effect assessments, and keep modern contractual protection for foreign processing, large businesses must build institutional systems.

d. **Capacity Building and Training –** To boost functional compliance, periodic staff training on privacy guidelines, breach reporting, and the risk of cross-border transfers should be established.

5.3 Future Directions

a. Effectiveness of the DPDP Act – Additional practical research needed to find out whether the DPDP Act really works in the real-world setting, particularly when it involves enforcement, user rights, and being able to work alongside other global data-protection systems.

b. **Interoperability Challenges –** Research in the future could examine how the GDPR and the DPDP Act differ, which makes it difficult to get data transferred easily across borders, and give suggestions on how to integrate these two sets of laws into a global or regional concord.

c. Impact on Digital Trade and Innovation – There is also a need for research to comprehend the monetary implications of various regulations and how they affect data-driven innovation, artificial intelligence progress, and digital trade.

d. **Organizational Compliance Behaviour –** The practical obstacles that industry stakeholders face while performing dual-system compliance across various jurisdictions can be identified with the comparative business studies.

6. Acknowledgments

The author would like to sincerely thank Dr. Yash Tiwari for her able guidance and constructive feedback during the writing of this article. The research's clarity and path both got direction by her valuable insights. The author also thanks Jagran Lakecity University for providing access to required study materials and a learning atmosphere.

7. Conclusion

Comparing the DPDP Act and the GDPR, this study concentrates on the way data stays secure when it is transmitted across borders. The results show that regulatory philosophy, business obligations, data subject rights, and means for foreign data flows are both comparable and distinct.

The GDPR provides strong protections, broad accountability requirements, and multiple routes for international data transfers through its rights-based structure. Large companies profit from their stable and clear regulatory framework, but it increases the difficulty of operations and expense The GDPR provides strong protections with broad accountability requirements, and multiple options for international data transfers through its structure centered around rights. Large companies profit from their stable and clear regulatory framework, but it increases the difficulty of operations and expenses (Voigt, & Von dem Bussche, 2017; Voss, 2022).

On the contrary, having a state-centric structure, with consent given high value consent , the DPDP Act provides specific duties for Significant Data Fiduciaries and unclear rules for cross-border transfers (Latham & Watkins LLP, 2023) . This method may make things easier for businesses worldwide; however, it could result in regulatory uncertainty and changes in integration (Latham & Watkins LLP, 2023).

Companies governed by both frameworks must manage competing compliance regimes by adopting enforcement systems to comply with varying guidelines and various cross-border data transfer regulations. The obligations provided by the GDPR as per the rights are just opposite to the inadequate data subject rights of the DPDP Act. This shows that systems of governance are required to mitigate variations in regulation and maintain privacy of data.

This study highlights as to why an integrated data transfer mechanism is necessary. The consent procedures, accountability standards, and data privacy must be synchronized. To improve the adherence to international privacy norms, Indian regulators ought to consider adding identical operational practices. Large companies must develop unified plans following strict rules of the GDPR along with the democratic requirements of the DPDP Act.

To conclude, the DPDP Act and GDPR have similar objectives of protecting privacy, accountability, and reducing risks, but they are very distinct in terms of design, operational requirements, and cross-border data transfer process. To facilitate participation in the global economy, boost digital services, and reinforce data privacy, it would be essential to overcome the gaps through standardized compliance practices, interoperable governance strategies, and constant regulatory discussion (Greenleaf, 2023; Voss, 2022).

References

Bowen, G. (2009). Document Analysis as a Qualitative Research Method. *Qualitative Research Journal*, *9*, 27–40. https://doi.org/10.3316/QRJ0902027

Braun, V., & Clarke, V. (2006). Using Thematic Analysis in Psychology. *Quantitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Bryman, A. (2016). *Social research methods* (Fifth edition). Oxford University Press.

Caron, P., Carr, B., Friedland, S. I., Goldberg, C., Goodenough, O., & Sprankling, J. (2015). THE CONTEMPORARY CIVIL LAW TRADITION: EUROPE, LATIN AMERICA, AND EAST ASIA. *LexisNexis Law School Publishing Advisory Board*. https://cap-press.com/pdf/9780820556765.pdf?srsltid=AfmBOop_qwT4Fa7sEZ0Xpd3KCAdQLL2vUyRBBsEikYyRThrQz3RSLEC3

Charter of Fundamental Rights of the European Union, Official Journal of the European Union § C 326/391 (2012). https://eur-lex.europa.eu/eli/treaty/char_2012/oj/eng

Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems v. Data Protection Commissioner (Case C-311/18) [Schrems II] (Court of Justice of the European Union (CJEU) 2020). https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=117724

Digital Personal Data Protection Act, 2023, Pub. L. No. Act no. 22 0f 2023, 21 (2023). https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf

European Commission. (2023). *Questions & Answers: EU-US Data Privacy Framework* [Text]. European Commission. https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3752

Greenleaf, G. (2021). *Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance* (SSRN Scholarly Paper No. 3836348). Social Science Research Network. https://doi.org/10.2139/ssrn.3836348

Greenleaf, G. (2023). *Global Data Privacy Laws 2023: 162 National Laws and 20 Bills* (SSRN Scholarly Paper No. 4426146). Social Science Research Network. https://doi.org/10.2139/ssrn.4426146

Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 ___ (Supreme Court of India 2017). https://indiankanoon.org/doc/91938676/

Kumar, D. (2025). BALANCING PRIVACY AND INNOVATION: ANALYZING THE DPDP ACT, 2023 IN INDIA'S CYBER LAW FRAMEWORK. *International Research Journal of Modernization in Engineering Technology & Science*.

Kuner, C. (2013). *Transborder Data Flows and Data Privacy Law* (Vol. 30). Oxford University Press.

Lakra, R., Kolanu, M., & Shrivastava, A. (2025). *Data, Control, and Power: Decoding India's Digital Personal Data Protection Act, 2023* (SSRN Scholarly Paper No. 5366868). Social Science Research Network. https://doi.org/10.2139/ssrn.5366868

Latham & Watkins LLP. (2023). *India's Digital Personal Data Protection Act, 2023 vs. The GDPR: A comparison*. https://www.lw.com/admin/upload/SiteAttachments/Indias-Digital-Personal-Data-Protection-Act-2023-vs-the-GDPR-A-Comparison.pdf

Nishith Desai Associates. (2023). *Nishith Desai Associates: The Firm*. Nishith Desai Associates. https://nishithdesai.com/research-and-articles/hotline/technology-law-analysis/indias-digital-personal-data-protection-act-2023-history-in-the-making-10703

OECD. (2022). *Measuring the value of data and data flows* (OECD Digital Economy Papers No. 345; OECD Digital Economy Papers, Vol. 345). https://doi.org/10.1787/923230a6-en

Press Information Bureau,. (2024). *Future Ready: India's Digital Economy to Contribute One-Fifth of National Income by 2029-30*. Government of India. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2097125

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 2016 O.J. (L 119) 1, Pub. L. No. Regulation (EU) 2016/679, 88 (2016). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legissum:310401_2#:~:text=MAIN%20DOCUMENT,is%20of%20documentary%20value%20only.

Solove, D. J. (2008). *Understanding Privacy* (SSRN Scholarly Paper No. 1127888). Social Science Research Network. https://papers.ssrn.com/abstract=1127888

Tufekci, Z. (2015). ALGORITHMIC HARMS BEYOND FACEBOOK AND GOOGLE: EMERGENT CHALLENGES OF COMPUTATIONAL AGENCY. *Colorado Technology Law Journal*, *13*. https://ctlj.colorado.edu/wp-content/uploads/2015/08/Tufekci-final.pdf

UNCTAD. (2021). *Digital Economy Report*. https://unctad.org/page/digital-economy-report-2021

U.S. Congress, Congressional Research Service. (2022). *U.S.–EU data transfers: Background and policy issues* (No. R46917). https://www.congress.gov/crs_external_products/R/PDF/R46917/R46917.3.pdf

Voigt, P., & Von dem Bussche, A. (2017). *The EU GDPR - A Practical Guide—Paul Voigt PDF | PDF | Information Privacy | Information Technology*. Scribd.

https://www.scribd.com/document/369822372/The-EU-GDPR-A-practical-Guide-Paul-Voigt-pdf

Voss, W. G. (2022). Cross-Border Data Flows, the GDPR, and Data Governance. *International Organisations Research Journal*, *17*(1), 56–95. https://doi.org/10.17323/1996-7845-2022-01-03

Zweigert, K., & Kötz, H. (1998). *Introduction To Comparative Law* (T. Weir, Trans.). Oxford University Press. https://www.scribd.com/document/371060999/An-Introduction-to-Comparative-Law-Zweigert-Ko-tz