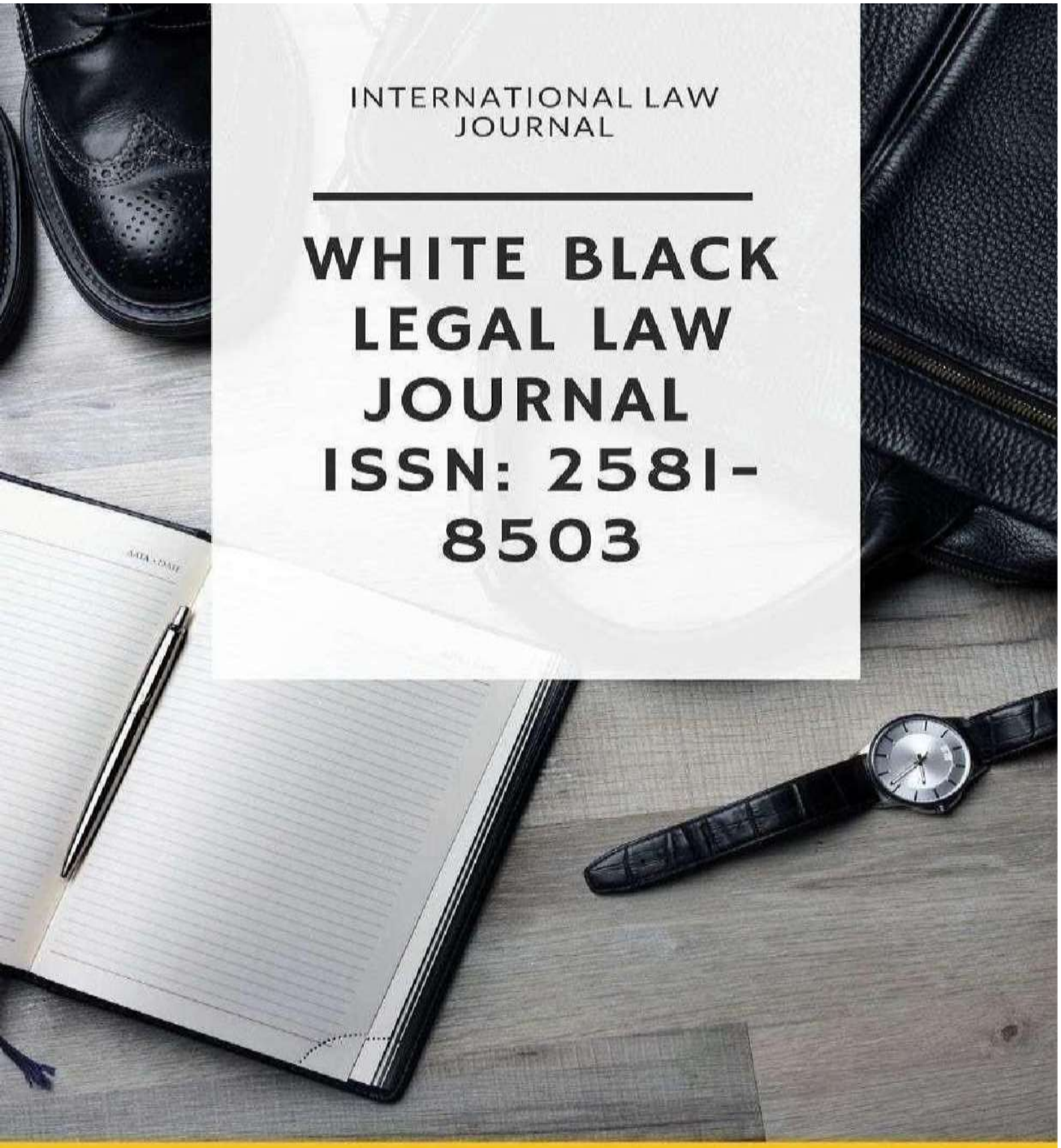

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

www.whiteblacklegal.co.in
Volume 3 Issue 1 | March 2025 ISSN: 2581-8503

ANALYSIS ON THE DATA PROTECTION REGULATIONS IN INDIA AND ITS COMPARISON WITH GDPR

AUTHORED BY - TAVISHI RASTOGI

Abstract:

Imagine navigating the digital world today – our lives increasingly intertwined with online services, apps, and platforms. In India, with its explosive digital growth, protecting our personal information has become paramount. The 2023 Digital Personal Data Protection Act[1] (DPDP Act) is India's response to this challenge, a new set of rules designed to keep our data safe. The Digital Personal Data Protection Act (DPDP Act) of 2023 represents India's legislative response to the escalating challenges of data privacy within its rapidly expanding digital economy. Aimed at balancing individual rights with the necessity of lawful data processing, the Act establishes a framework for handling digital personal data, emphasizing consent and accountability. This research undertakes a comprehensive analysis of the Act, delineating its core provisions, enforcement mechanisms (including the Data Protection Board), and consequential implications for both individual data subjects ("Data Principals") and organizational data processors ("Data Fiduciaries"). It explores key aspects such as data minimization, purpose limitation, privacy notices, and breach reporting obligations. A comparative study is subsequently conducted, placing the DPDP Act with the European Union's General Data Protection Regulation[2] (GDPR), a benchmark for global data protection standards. The analysis highlights areas of convergence and divergence, considering factors like the scope of protected data, consent requirements, penalties for non-compliance, and exemptions granted under each regime. The research also addresses criticisms and potential challenges in implementing the DPDP Act, such as enforcement capacity and the breadth of governmental exemptions. Ultimately, this paper contributes to understanding how India's data protection framework aligns with international norms and identifies opportunities to strengthen its effectiveness in safeguarding digital privacy for its citizens.

[1] The Digital Personal Data Protection Act, 2023 (India)
[2] Regulation 2016/679, General Data Protection Regulation (GDPR), 2016 O.J. (L 119) 1 (EU)

Introduction:

The exponential growth of digital technologies has revolutionized how personal data is collected, stored, and processed. From social media platforms to e-commerce websites, individuals constantly share their personal information online, often without fully understanding how it is used or protected. This has led to growing concerns about privacy breaches and misuse of sensitive information. Recognizing the need for robust legal frameworks to address these challenges, countries worldwide have implemented comprehensive data protection laws.

In India, the journey toward effective data protection began with the recognition of privacy as a fundamental right in the landmark Justice K.S. Puttaswamy[3] case in 2017. This paved the way for legislative efforts culminating in the Digital Personal Data Protection Act (DPDP Act) of 2023. The DPDP Act is designed to strike a balance between protecting individual privacy rights and enabling lawful data processing for economic and administrative purposes. It introduces key provisions such as consent-based processing, rights for data principals (individuals), obligations for data fiduciaries (entities handling personal data), and penalties for non-compliance.

Globally, the European Union's General Data Protection Regulation (GDPR), enforced since 2018, has set a benchmark for data protection laws with its stringent requirements and extraterritorial applicability. While India's DPDP Act shares some principles with GDPR, it also diverges in significant ways due to differences in socio-economic contexts and policy priorities.

This paper aims to analyse India's DPDP Act comprehensively while comparing it with GDPR to understand their respective strengths and limitations. By exploring this comparative framework, we seek to uncover lessons from GDPR that can inform improvements in India's approach to data protection and foster alignment with global standards[4].

These sections are written in a humanized tone while maintaining academic rigor. They provide a clear overview of your topic and set the stage for deeper analysis in subsequent sections of

[3] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India)
[4] Daniel J. Solove, *Comparing Data Protection Laws: GDPR and India's Data Protection Framework*, Int'l Data Protection & Privacy L. Rev. (2020).

your research paper.

Background and Context:

The evolution of data privacy laws in India reflects the nation's journey into the digital age. Before the Digital Personal Data Protection Act (DPDP Act) of 2023, India's legal framework for data protection was primarily governed by the Information Technology Act, 2000, along with its Section 43A, which provided limited protection for sensitive personal data. However, the landmark ruling by the Supreme Court in the Justice K.S. Puttaswamy case (2017) declared privacy a fundamental right, underscoring the need for a comprehensive data protection law. This ruling catalysed the development of the Personal Data Protection Bill in 2019 (PDPB 2019), modelled after global data privacy laws. The PDPB 2019 aimed to establish standards for cross-border data transfers and accountability for entities processing personal data[5]. However, it faced significant criticism, particularly regarding social media regulation and data localization requirements. Consequently, amendments were proposed in 2021 (DPB 2021), but the bill was eventually withdrawn in August 2022 due to international standards and upcoming challenges. The Digital Personal Data Protection Bill 2022 (DPDP 2022) was then released, leading to the enactment of the DPDP Act in August 2023.

In contrast, Europe's approach to data protection has deeper historical roots. The European Convention on Human Rights (1950) laid early groundwork, followed by the Data Protection Directive 95/46/EC in 1995. These initiatives reflected a growing awareness of privacy as a fundamental right in the face of increasing data processing capabilities. However, the need for a more unified and enforceable framework led to the development of the General Data Protection Regulation (GDPR), which came into effect in May 2018. GDPR aimed to harmonize data protection laws across the EU, empowering individuals with greater control over their personal data and imposing strict obligations on organizations processing data[6]. GDPR's extraterritorial scope also extended its influence beyond Europe, impacting organizations worldwide that process the data of EU residents.

[5] Ram Govind Singh & Sushmita Ruj, *A Technical Look at the Indian Personal Data Protection Bill*, (2020)
[6] Nehaa Bhandari & Gautam Bhatia, *Data Protection and Privacy: Indian and Global Perspectives*, J. Cyber L. & Pol'y (2022).

Overview of DPDP Act:

India's Digital Personal Data Protection Act (DPDP Act) of 2023 governs the processing of digital personal data within India. Its key features include its applicability to personal data collected in digital form or digitized subsequently, excluding data processed for personal or domestic purposes or made publicly available by the data subject or under legal authority. The Act has an extraterritorial scope, covering data processing outside India if it relates to offering goods or services to individuals in India.

Key definitions under the DPDP Act include:

- **Data Fiduciary:** Any person who determines the purpose and means of processing personal data.
- **Data Principal:** The individual to whom the personal data relates.
- **Data Processor:** Any person who processes personal data on behalf of a data fiduciary.
- **Consent Manager:** One who enables Data Principals to give, manage, and withdraw consent.
- **Significant Data Fiduciary:** A data fiduciary notified by the Central Government due to factors like the volume and nature of personal data processed.

The DPDP Act emphasizes consent as a critical ground for lawful data processing, allowing Data Principals to rectify or withdraw their consent at any time. It also includes specific exemptions for government activities, startups, and processing activities in the interest of national security or public order.

Data Fiduciaries have several duties under the Act, including:

- **Data Minimization:** Collecting only necessary data for a specific purpose.
- **Purpose Limitation:** Using data only for the purpose for which consent was given.
- **Privacy Notice:** Providing clear and accessible privacy notices in English and other languages listed in the 8th schedule of the Indian Constitution.
- **Consent:** Obtaining verifiable consent from Data Principals or their legal guardians.
- **Data Accuracy:** Ensuring the accuracy, completeness, and consistency of processed personal data.
- **Security Measures:** Implementing necessary security measures to prevent data breaches.
- **Redressal Mechanisms:** Providing effective and convenient redressal mechanisms for grievances.

- **Breach Reporting:** Reporting data breaches to the Data Protection Board and affected individuals within a reasonable time.

The Act prohibits tracking, behavioural monitoring, and targeted advertising of children, unless permitted by the government, and emphasizes the use of simple language and minimal cross-referencing for ease of understanding ("SARAL"). The Data Protection Board (DPB) serves as the enforcement authority, with the Telecom Disputes Settlement and Appellate Tribunal as the appellate authority[7].

Overview of GDPR:

The General Data Protection Regulation (GDPR) is a comprehensive data protection law that came into effect in May 2018, harmonizing data protection laws across the European Union (EU) and the European Economic Area (EEA). GDPR's key principles include lawfulness, fairness, and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality; and accountability.

GDPR applies to the processing of personal data, defined as any information relating to an identified or identifiable natural person ("data subject"). It has a broad territorial scope, applying to organizations established in the EU and those processing the personal data of EU residents, regardless of their location.

GDPR grants several rights to data subjects, including:

- **Right to Access:** The right to obtain confirmation of whether their data is being processed and access to that data.
- **Right to Rectification:** The right to correct inaccurate or incomplete personal data.
- **Right to Erasure ("Right to be Forgotten"):** The right to have personal data erased under certain circumstances.
- **Right to Restriction of Processing:** The right to limit the processing of personal data under certain conditions.
- **Right to Data Portability:** The right to receive personal data in a structured, commonly used, and machine-readable format.
- **Right to Object:** The right to object to the processing of personal data.

GDPR imposes obligations on data controllers (entities determining the purposes and means of

[7] CyberPeace Foundation, *Prohibition of Behavioral Tracking and Targeted Advertising for Children Under the DPDP Act 2023* (2023)

processing personal data) and data processors (entities processing data on behalf of controllers). These obligations include implementing appropriate technical and organizational measures to ensure data security, conducting data protection impact assessments (DPIAs) for high-risk processing activities, and appointing a Data Protection Officer (DPO) under certain circumstances.

GDPR's enforcement mechanism involves supervisory authorities in each EU member state, who have the power to investigate and impose fines for non-compliance. Penalties for GDPR violations can be severe, reaching up to €20 million or 4% of the organization's global annual turnover, whichever is higher.

Comparative Analysis: The Digital Personal Data Protection Act (DPDP) of India and the General Data Protection Regulation (GDPR) of the European Union are two comprehensive frameworks aimed at protecting personal data, but they differ significantly in scope, consent requirements, enforcement mechanisms, and other key aspects[8].

- **Scope and Definition:**

  The DPDP Act focuses exclusively on digital personal data, reflecting India's emphasis on a digital-first approach. It applies to all organizations processing personal data of individuals located in India, regardless of the organization's location. In contrast, GDPR covers both digital and non-digital formats of personal data, offering a broader definition that includes any information capable of identifying an individual. GDPR applies globally to organizations processing data of EU residents, irrespective of their geographic location. This expansive scope ensures comprehensive protection for EU citizens but imposes additional compliance burdens on international businesses.

- **Consent and Individual Rights**

  Consent plays a central role in both laws but is applied differently. The GDPR requires explicit consent for processing personal data, with limited exceptions such as contractual necessity or public interest. It also grants individuals extensive rights, including access to their data, erasure (the "right to be forgotten"), data portability, and the ability to object to automated decision-making or restrict processing. The DPDP Act emphasizes consent but allows broader exemptions for government functions and

[8] Observer Research Foundation, *Data Protection in India: A Comparative Analysis with GDPR* (2023)

legitimate uses, which may dilute individual control over personal data. While it provides rights such as rectification and withdrawal of consent, it lacks some of the comprehensive protections offered by GDPR.

- **Enforcement Mechanisms**

  Enforcement structures vary significantly between the two frameworks. The DPDP Act is overseen by India's centralized Data Protection Board (DPB), which handles compliance monitoring and grievance redressal. On the other hand, GDPR employs a decentralized approach with Supervisory Authorities in each EU member state responsible for enforcement. This structure allows for localized governance tailored to regional contexts. Penalties under both laws are steep: the DPDP Act imposes fines up to ₹250 crores (approximately €28 million), while GDPR allows penalties up to €20 million or 4% of global annual turnover—whichever is higher—making it one of the most stringent privacy laws globally.

- **Data Transfers and Localization**

  Cross-border data transfer regulations differ markedly between the two frameworks. GDPR enforces strict mechanisms such as Standard Contractual Clauses or Binding Corporate Rules to ensure adequate protection when transferring personal data outside the EU. It also restricts transfers to countries deemed inadequate in terms of data protection standards[9]. The DPDP Act does not mandate strict localization but enables the Indian government to restrict transfers to certain notified countries or territories. This approach is less prescriptive than GDPR but relies heavily on governmental discretion.

- **Data Breach Notifications**

  Both laws require organizations to report data breaches promptly, but their requirements differ. GDPR mandates notification to Supervisory Authorities within 72 hours of becoming aware of a breach, emphasizing urgency in addressing violations. The DPDP Act similarly requires reporting breaches to the DPB and affected individuals but does not specify a strict timeframe like GDPR, potentially leading to

[9] Anirudh Burman, *Understanding India's New Data Protection Law*, Carnegie Endowment for International Peace (2023)

delays in breach mitigation.

- **Principles-Based vs Rules-Based Approach**

  The DPDP Act adopts a principles-based framework that offers flexibility in implementation but may lead to inconsistencies in enforcement. In contrast, GDPR provides detailed rules and guidelines that ensure clarity and consistency across jurisdictions but impose higher compliance[10] burdens on organizations. For instance, GDPR includes special categories of sensitive personal data with stricter processing conditions, while DPDP applies uniformly across all types of digital personal data without additional controls for sensitive or critical categories.

- **Additional Differences**

  GDPR imposes stricter conditions on processing children's data and includes provisions for automated decision-making objections. It also requires organizations to document their data processing activities comprehensively. The DPDP Act has fewer specific requirements in these areas but introduces higher flexibility for innovation and growth within India's digital economy.

  While both laws aim to protect personal data and empower individuals with rights over their information, GDPR adopts a more stringent rules-based approach with broader scope and detailed protections, whereas DPDP focuses on flexibility tailored to India's digital-first economy. These differences reflect distinct regulatory philosophies shaped by regional priorities and economic contexts

Implications for Stakeholders:

The Digital Personal Data Protection Act (DPDP) of India and the General Data Protection Regulation (GDPR) of the European Union have profound implications for various stakeholders, including businesses, individuals, and governments.

For **businesses**, compliance with these regulations necessitates significant changes in how they collect, store, and process personal data. Under the DPDP Act, companies must invest in new technologies and processes to ensure compliance[11], which can lead to increased operational

[10] KPMG, *India's Data Protection Regime: Understanding Compliance with DPDP & GDPR* (2023)
[11] PwC India, *GDPR vs. DPDP Act: Compliance Challenges for Indian Businesses* (2023)

costs. This includes hiring data protection officers, conducting regular audits, and implementing robust cybersecurity measures to protect customer data. While these requirements may seem burdensome initially, they can ultimately enhance a company's reputation by fostering consumer trust. Adopting responsible data management practices can differentiate businesses in a competitive market, enabling them to attract consumers who prioritize privacy and security.[12]

Individuals stand to benefit significantly from these regulations as they empower users with greater control over their personal information. The DPDP Act grants rights such as access to personal data, the ability to correct inaccuracies, and the right to withdraw consent for data processing. These provisions enhance individual autonomy and promote transparency in how personal data is handled. As consumers become more aware of their rights, they may demand higher standards of accountability from businesses, leading to a more privacy-conscious culture. However, individuals also face challenges; they need to navigate complex consent mechanisms and understand their rights under these regulations, which can be overwhelming without proper guidance.

For **governments**, both the DPDP Act and GDPR represent a commitment to safeguarding citizens' privacy while fostering innovation in the digital economy. By establishing clear legal frameworks for data protection, governments can mitigate risks associated with data breaches and misuse of personal information. This not only protects citizens but also enhances national security by regulating how sensitive information is managed[13]. Furthermore, these regulations can attract foreign investment by demonstrating a commitment to high standards of data protection. By ensuring that businesses comply with these laws, governments can create an environment conducive to growth while maintaining public trust.

Conclusion:

In today’s digital age, where personal and professional interactions are increasingly mediated by technology, the regulation of data privacy has become a necessity rather than a choice. The Digital Personal Data Protection Act (DPDP Act) of 2023 marks a pivotal moment in India’s journey toward safeguarding personal information while fostering a thriving digital

[12] Internet Freedom Foundation, *The Future of Data Privacy in India: Challenges and Opportunities*

economy. Similarly, the General Data Protection Regulation (GDPR) in the European Union has set a global precedent, offering a robust framework for data protection that has influenced policies worldwide.

India's DPDP Act reflects its unique socio-economic priorities, adopting a principles-based approach that provides flexibility for businesses and government entities to process data responsibly. This flexibility is particularly suited to India's rapidly growing digital-first economy, where innovation and accessibility are critical. In contrast, GDPR enforces strict and detailed regulations, ensuring comprehensive protections for individuals but imposing significant compliance obligations on organizations. This divergence underscores the differing policy priorities of the two jurisdictions: India emphasizes economic growth and digital innovation, while the EU focuses on stringent privacy rights and regulatory uniformity[14].

Both frameworks share common ground in areas such as consent-based data processing, accountability, and breach notification requirements. However, they differ significantly in their scope, enforcement mechanisms, and exemptions. For instance, GDPR applies to both digital and non-digital personal data globally, while the DPDP Act is limited to digital personal data with certain exemptions for government functions and national security concerns. GDPR's decentralized enforcement through Supervisory Authorities contrasts with India's centralized Data Protection Board (DPB) model.

These laws also have far-reaching implications beyond legal compliance. For businesses, they present challenges in adapting to new standards but also opportunities to build trust with consumers by demonstrating a commitment to privacy. For individuals, these regulations empower them with greater control over their personal information, fostering transparency and accountability in how their data is handled. Governments benefit from structured frameworks that enhance oversight while enabling international cooperation on data protection issues.

The DPDP Act represents a critical milestone in India's digital transformation journey. While still evolving, it aligns with global trends and lays the groundwork for a more secure and

[14] *The Digital Personal Data Protection Act, 2023*, No. 22 of 2023, India Code (2023)

privacy-conscious digital ecosystem[15]. By learning from GDPR's successes and addressing its own unique challenges—such as enforcement capacity and balancing governmental exemptions—India has the potential to strengthen its data protection framework further.

Ultimately, both the DPDP Act and GDPR illustrate how nations can navigate the complex interplay between privacy, innovation, and governance in an increasingly interconnected world. As technology continues to advance at breakneck speed, these frameworks remind us of the importance of protecting individual rights while enabling progress—a balance that will shape the future of data protection worldwide.

[15] *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 (General Data Protection Regulation)*, 2016 O.J. (L 119) 1