



International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Comparative Study on GDPR and DPDP, Act

Sri Savithri Subbiah¹, A.Shanmuga Priyanga²

¹4th year B.com LL.B. (Hons), Chettinad School Of Law, Kelambakkam, Tamil Nadu, India.

²4th year B.com LL.B. (Hons), Chettinad School Of Law, Kelambakkam, Tamil Nadu, India.

ABSTRACT

In today's technological driven society, personal data is so precious and protecting one's personal data has become a legal and challenge. Protecting the personal data of an individual is connected with fundamentals rights of the citizen. The European Union's General Data Protection Regulation (GDPR) started in May, 2018. It applies to the European Economic Area (EEA), which includes all 27 EU member states along with Iceland, Liechtenstein, and Norway. In total 30 countries, provided a legal baseline for data protection. Similar to this, India also passed a Digital Personal Data protection Act (DPDP) 2023, to protect the citizen's digital rights.

This study is a comparative examination of GDPR and DPDP Act, The GDPR takes a strict, rights-focused approach with rules like data portability, the right to be forgotten, and even applying beyond the EU. In contrast, India's DPDP Act is shaped more by the country's own social, economic, and technological needs as it builds its digital economy. Overall, the DPDP Act focuses on consent- based processing of data, prevention of misuse, and accountability of data fiduciaries, acknowledging fewer explicit rights than those enshrined in the GDPR.

This study will compare these two legal structures and provide key comparative analysis of the provisions of each law, whom they apply to, focusing on scope, applicability, principles to be followed, rights of individuals, duties of data processors and fiduciaries, issues regarding enforcement. By assessing similarities and differences in the GDPR and DPDP, businesses can better understand the developments of global data protection compliance. As well as explaining the challenges in implementing the DPDP act in India which also includes the institutional capacity, awareness, compliance costs and balancing privacy with economic development

Key words: Right to privacy, DPDP Act, Article 21, Right to be forgotten, Sensitive personal data, Penalties and liabilities, Regulatory Authorities.

1. Introduction

The digital development that is currently taking place in our economy has changed everything including human interactions (in person interactions to through mobile phones), commerce (physical buying selling from stores directly to e-commerce), governance (to e-governance). Due to rise in internet usage, social media platforms, artificial intelligence, etc... and vast amount of data are generated, collected and processed daily. These technological advancement bring enormous benefits as well as drawbacks and poses high risk to privacy and human dignity so there is a need to protect the digital data and safeguard the individuals right.

All around the world, protecting personal data has become an key issue in law and policy. The European Union introduced the General Data Protection Regulation (GDPR) in 2018. This law not only gives people stronger control over their personal data it also focuses on companies and government bodies. What makes GDPR unique is that it applies even to companies outside Europe if they deal with the data of EU citizens.as a result, GDPR is now seen as a global model for privacy laws.

India has moved slowly in developing its data protection framework. The Information technology Act, 2000 which majorly focusses on cybercrimes and e-commerce and contained very limited provisions relating to personal data. The SPDI (Sensitive personal Data or Information) Rules, 2011 which lays down basic requirement for how organizations should handle sensitive data. These were issues under Section 43A of information Technology Act, 2000. A major significant shift took place in 2017, where privacy is recognised as a fundamental right in the case of "K.S.Puttuswamy v. Union of India". This case lead to the drafting of Personal Data Protection Bill, 2018 by Justice B.N.Srikrishna committee, which underwent several revisions. Later it was finally enacted as the DPDP (Digital Personal Data Protection) Act, 2023.

The DPDP Act aims to focus on the protection of personal data as well as the growth of India's digital economy. While GDPR has narrow coverage, fewer individual rights and wider exemptions for government bodies. It is therefore essential to analyze the DPDP Act in relation to global best practices to understand similarities and differences.

2. Research Questions

- 1) What are the difference between the GDPR and DPDP act in terms of rights of the individual whose data is collected and the responsibilities of the one who collects and process the data?
 - 2) What are the scope, applicability and legal grounds for processing personal data under GDPR and DPDP act?
 - 3) How do enforcement mechanism and regulatory authority differ with regard to independence, power and effectiveness under GDPR and DPDP act?
-

3. Objectives

- 1) To compare the GDPR and the DPDP Act in terms of their structure, main principles, scope, applicability and legal grounds for processing data rights and how they protect personal data.
 - 2) To study rights given to individuals and the duties placed on organizations that collect or use personal data.
 - 3) To review how enforcement bodies work under both laws, focusing on their independence, powers, and effectiveness.
 - 4) To suggest ways to improve India's DPDP Act and bring it closer in line with global best practices.
-

4. Statement of problem

With the growth of rapid digitalisation the collection and use of personal data have grown enormously. Though this brings a lot of opportunity to individuals, it is also serious legal and ethical question about privacy, fairness, and accountability. EU is considered as the golden standard for safeguarding the privacy and data. EU is basically a developed country and India is still a developing country so the law which is designed by EU in its own context is not easy to adopt in developing countries like India, there arises the need for DPDP act.

India's new Digital Personal Data Protection (DPDP) Act is a big step in the right direction. It shows that India is serious about protecting personal data. Yet, important differences remain when we compare it with the GDPR—especially around individual rights, procedural safeguards, and the scope of government powers.

5. Research Methodology:

The research methodology adopted for this research paper is doctrinal research. This involves studying and comparing of the GDPR and DPDP act, it is a qualitative comparative legal analysis, supported by academic articles and commentaries. This paper majorly focuses on analysing key areas such as scope, individual rights, data fiduciary obligations, enforcement, and regulatory frameworks. This approach helps to identify the differences and similarities of UE and india in data protection policy and practice. Alongside, a comprehensive review of secondary sources like government report, and case studies. This approach gives a holistic understanding of the comparative regulatory landscape of data protection in a rapidly digitizing world.

6. Literature review:

1. DPDP Act 2023 vs. GDPR: A Comparative Analysis of India's & EU's Data Privacy Law.

By Pameela George Puthenveeti (2024),

(The DCU Law & Tech Research Cluster)

This article highlights the significance and important step in India's data protection, also focusing on data localization, user consent, fiduciary accountability and digital autonomy as well. This paper also provides a clear comparison showing the difference in rights, obligations, and enforcement. But it is more descriptive than analytical with only few example. Few points were repeated and the scope is narrow. Overall this paper lacks in enforcement, cross border data flow issues, SME impact which require further research.¹

2. Comparative analysis of GDPR and digital personal data protection act, 2023

By Hemalatha G. and Saikrupaa K. (2023)

ISSN: 2320-2882 (Indian Journal of Law and Legal Research)

¹Pameela George Puthenveeti, DPDP Act 2023 vs. GDPR: A Comparative Analysis of India's & EU's Data Privacy Law, The DCU Law & Tech Research Cluster, (2024)

This article compares India's DPDP act with EU's GDPR act. Both aim to protect personal data but the scope, rights, enforcement differs. The limitation in this paper is that this has limited critical evaluation and practical examples of enforcement or challenges. The main research gap is the lack of discussion on implementation challenges in india, also the author need to highlight the need for stronger data protection measures.²

3. The right to be forgotten: A comparative analysis of the GDPR and the DPDP Act

By Bhargav Chaganti (2024)

ISSN: 2320-2882 (Indian Journal of Law and Legal Research)

This article compares the right to be forgotten under GDPR and DPDP act. This paper gives detailed analysis of article 17 GDPR, also explains the balance between privacy, freedom of expression, and public interest. The research gap in this paper is the lack of clarity on how right to be forgotten will function in practice in india, regarding conflicts with right to information and freedom of speech, technical enforcement challenges, and the absence of comprehensive safeguards compared to GDPR.³

4. Assessing india's digital personal data protection Act, 2023: A comparative study with GDPR.

By Vaibhav Dharod and Kevin Tauro (2023)

ISSN: 2582-8878 (Indian Journal of Law and Legal Research)

The work of Vaibhav Dharod and Kevin Tauro emphasizes the significance of data security in the digital era and offers a distinct comparative examination of the GDPR and India's DPDP Act, 2023. Its advantages include clarifying user rights, fiduciary duties, historical background, and fundamental principles of both laws, rendering the study pertinent and thorough. Nonetheless, the study presents shortcomings in investigating real-world enforcement issues, the autonomy of India's Data Protection Board, extensive government exemptions, and the vague structure for international data transfers. It also does not completely assess the effects of the Act on children and at-risk populations. These gaps indicate a requirement for additional investigation into implementation and protections to guarantee the DPDP Act aligns with international benchmarks⁴

5. "Critical Analysis: Digital Personal Data Protection Bill 2022"

Bashambu and Chetwani (2022),

published in *Jus Corpus Law Journal*,

The extant writings indicate that the GDPR along with India's DPDP Act, 2023 are steps taken in the right direction for protection of individual rights over his or her data particularly with respect to cross-border transfer of data, consent and the privacy right. Academics acknowledge that the DPDP Act aligns India more with international norms and makes it easier for individuals to manage their own data. But this research paper also lacks problematic gaps, such as weaker enforcement compared to the GDPR, lack of precision around what constitutes sensitive personal information and worries about notions like "deemed consent." Moreover, the majority of works are purely legal comparisons, while there is little investigation that directly addresses practical obstacles to implementation, including data leakages during COVID-19. This adds ground for a more in-depth study of the enforcement and efficacy of the Act in India when it comes to digital framework.

6. The digital personal data protection Act, 2023: A legal analysis in light of global data protection standards by Prabhash Dalei (2025) International Journal of Law Volume and Issue: Volume 11, Issue 3, 2025, Pages 127-131 ISSN: 2455-2194⁵

paper "The digital personal data protection Act, 2023: A legal analysis vis a vis global data protection standards" by Prabhash Dalei (2018), published in the International Journal of Law (ISSN 2455-2194) Vol.1 No.2 is critical to India's DPDP Act as it compares it with EU's GDPR. It emphasizes the discipline of consent and transparency, accountability and child protection built into the DPDP Act to further India's digital economy. However, DPA identifies shortcomings including DPDP's restriction to digital data alone, lack of right to portability of data and wide government exceptions without adequate judicial involvement, and almost loose cross border transfer regime. The study recommends the resolution of these problems, proposes some reforms to regulatory independence and aspires for a more balanced and internationally compatible system of data protection.

²Hemalatha G. and Saikrupaa K., *Comparative analysis of GDPR and Digital Personal Data Protection Act, 2023*, Indian Journal of Law and Legal Research (ISSN: 2320-2882), (2023)

³Bhargav Chaganti, *The Right to be Forgotten: A Comparative Analysis of the GDPR and the DPDP Act*, Indian Journal of Law and Legal Research (ISSN: 2320-2882), (2024)

⁴Vaibhav Dharod and Kevin Tauro, *Assessing India's Digital Personal Data Protection Act, 2023: A Comparative Study with GDPR*, Indian Journal of Law and Legal Research (ISSN: 2582-8878), (2023)

⁵Prabhash Dalei, *The Digital Personal Data Protection Act, 2023: A Legal Analysis in Light of Global Data Protection Standards*, International Journal of Law (Volume 11, Issue 3, ISSN: 2455-2194). (2025)

7. Overview of GDPR and DPDP Act

The digital data protection regulation (GDPR), enforced in the European union since May 2018. It is considered as the most comprehensive data protection law in the world. It regulated the processing of personal data by controllers and processors both within and outside EU. It is based on the principle of fairness, transparency, accountability. It grants individual extensive rights like access, correction, erasure, profitability and objection to processing. Organisation must report any breaches within 72 hours. Enforcement of this is carried out by independent supervisory authorities, with penalties reaching upto 20 euro million or 4 % of global annual turnover, making GDPR a global benchmark for privacy governance.

India's Digital Personal Data Protection Act, 2023 (DPDP) is the country's 1st dedicated data protection law. It applies to digital personal data, including the data collected online and extends to entities outside india offering goods and services to Indian residents. The Act defines of data principle (individuals), data fiduciary (controller) and data processor. The act also grants access, correction, erasure and consent withdrawal, while imposing obligations of accountability, transparency and security on fiduciaries. Unlike GDPR act, it excludes non-digital data and gives broader exemption for government entities. Enforcement Lies with the newly established Data Protection Board of India, while the penalties are monetary but less stringent than GDPR's fines.

DPDP Act is inspired by GDPR, but DPDP Act diverges in scope, coverage and enforcement. While GDPR sets a global standard, India's DPDP Act is more flexible, context specific approach in balancing privacy with the state and economic interest.

8. Comparison of GDPR and DPDP Act:

1. Rights of individuals and responsibilities of organisations:

1.1 Rights of individuals:

Both these acts revolves around the rights of individuals whose data is collected and the responsibilities of the organisation who collects and process the data. They aim to create a legal framework that balances these interest but they differ in scope, depth and enforcement.

Under the GDPR, individuals ar refered as data subjects. They have the right to access their data, request rectification of inaccuracies, demand erasure (right to be forgotten), restrict or object to processing, and request data profitability. The Act protects the individual from automated decisions-making and profiling that greatly affects them. The rights of individuals provided under this act are based on the principle of transparency, fairness and accountability. This act ensures that individuals can exercise their rights without undue barriers. The act requires the organisations respond to data subject requests promptly, typically within one month and imposes strict obligations and facilitate these rights⁶

The DPDP Act, gives the rights on data principals that are comparatively narrower in scope. Individuals can access information about the personal data held about them, request correction or completion, withdraw consent and seek erasure (right to be forgotten), they also have right to grievance redressal. The DPDP Act does not explicitly provide for data portability. There are also some exemptions that applies to the government entities, especially in areas related to sovereignty, security and public order. Hence the scope of the individual rights under DPDP is limited than GDPR, particularly when the data in not in digital form.⁷

1.2 Responsibilities of organisations

GDPR gives certain obligations on data controllers and processors, emphasizing accountability and proactive compliance. The organisations must implement privacy by design and by default, maintain records of processing activities, conduct Data Protecton Impact Assessment (DPIAs) when processing high risk and ensures the data is secure, accurate and processed lawfully. Controllers must obtain unambiguous consent. Organisations must report within 72 hours of breach and may face penalty of up to 4% of their global annual turnover or euro 20 million, whichever is higher. GDPR mandates that organisations establish a proactive compliance culture and implement a strong data governance framework⁸

The DPDP Act imposes responsibilities on data fiduciaries and processors. The organisations must ensure lawful processing, maintain transparency and implement security safeguards. They must also establish grievance redressal mechanisms, and allow individuals to use their rights. The Act requires that consent must be free, and informed along with the ability to withdraw at any time. The DPDP Act provides broader exemptions for certain categories of processing, especially by government entities. At the same time data fiduciaries are accountable for breaches and non-compliance. The enforcement and penalty is less compared to GDPR

1.3 Comparative insights

Both the Act GDPR and DPDP emphasize the principle of consent-based processing and grants individuals rights to access, correct and erase their personal information. They also places an obligations on organisations to process data lawfully, securely and more transparently. GDPR offers broader rights while DPDP provides narrower rights including data portability. GDPR enforces stringent requirements while DPDP act is more flexible.

⁶ Regulation (EU) 2016/679, arts. 12-22, 24-25; Digital Personal Data Protection Act, 2023, sec 3-5, 18-19 (India),

⁷ GDPR Regulation (EU) 2016/679, arts. 12-20; Information Commissioner's Office, The Rights of Individuals (Nov. 18, 2024)

⁸ Regulation (EU) 2016/679, arts. 24-25, 33, 83; Digital Personal Data Protection Act, 2023, §§ 18-23 (India), (Aug 31, 2025)

Both laws aim to protect individual privacy. GDPR provides more framework with far-reaching rights and obligations, While the DPDP Act provides legal recognition to data privacy and setting up a regulatory framework. Individual rights, organisational accountability and enforcement mechanisms may be required to align it more closely with global best practices.⁹

2. Scope, Applicability and legal grounds for data processing

2.1 Territorial and Functional Scope of GDPR and DPDP Act

The GDPR has a vast territorial scope, extending to organizations within the European Union as well as those outside the EU in case they process personal data in relation to providing goods or services to data subjects within the EU or keeping tabs on their behavior. It regulates both data processors and data controllers, holding them accountable within the data landscape. Significantly, GDPR applies to online and offline means of collection and processing of personal data and is therefore functionally extensive. The DPDP Act, 2023 of India, in contrast, applies only to digital personal data and mainly to in-country processing. Nevertheless, similar to GDPR, it too has an extraterritorial reach over entities located outside India if they process digital data of Indian individuals for goods or services. Functionally, the DPDP Act is applicable to data fiduciaries and processors, but its compliance architecture is easier than that of GDPR, with an emphasis on more general obligations rather than prescriptive procedural rules.

2.2 Types of personal data covered under each law

The GDPR Act has a broad approach towards personal data. This act defines personal data as any information that directly or indirectly identify an individual like names, identification numbers, location data or online identifiers. GDPR recognises "special categories of personal data" which includes information related to race, origin, political opinion, religious belief, trade union membership, health, biometric or genetic data and data related to sex life of a person or sexual orientation. Since these are sensitive details, more stringent rules are applicable, and such data may only be utilized under specific ascertainable conditions.

The DPDP Act does not, however, create such categories. It defines personal data widely as data about an identifiable individual but applies all personal data under a single regulatory regime. Rather than defining special categories, it creates the notion of Significant Data Fiduciaries (SDFs), which are organizations the government identifies based on the size, sensitivity, and risks of their data processing operations. Such organizations have to adhere to heightened responsibilities, thus indirectly recognizing varying degrees of data sensitivity.

2.3 Legal grounds for processing personal data

The GDPR provides a detailed framework of six legal basis for processing personal data:

- (1) Freely given, informed, specific, and unambiguous consent;
- (2) Processing required for the performance of a contract;
- (3) Fulfilling a legal obligation under EU or Member State law;
- (4) Safeguarding important rights of the data subject or of another natural person;
- (5) Carrying out tasks in the public interest or of official authority; and
- (6) Pursuing legitimate interests of the controller or of third parties, as long as such interests do not prejudice the rights and freedoms of individuals. This broad spectrum of legal bases enables organizations to process personal data on strictly prescribed conditions, balancing business requirements with individuals' rights. The DPDP Act streamlines this approach by acknowledging two broad categories: consent and deemed consent. Consent should be voluntary, informed, particular, unconditional, and withdrawable at any moment by the data principal. Deemed consent, in contrast, allows for processing without express consent under specific circumstances like compliance with the law, state functions, medical emergencies, employment, and other "fair and reasonable purposes" as notified by the government. While GDPR establishes a more detailed and restrictive model, the DPDP Act indulges in a flexible, state-centered paradigm, depending more on deemed consent to facilitate easier administration and provision of services.¹⁰

3. Enforcement mechanism and regulatory Authorities

3.1 Independence, Powers and effectiveness of Regulatory Authorities

Under the GDPR, the enforcement is carried out by independent supervisory authorities (SAs) in each EU member state. These enforcement authorities are legally accountable to national parliaments, they ensure that operates they operate free from undue external influence. SAs have wide range of powers including the ability to investigate complaints, conducting audits, issuing warnings, order suspension of data processing and mandates corrective measures. The further enhancement would be found in the coordination between SAs and EDPB as stipulated under the GDPR, with the result that there will be harmonized GDPR interpretation within the EU.

While the DPDP Act, 2023, erected the Data Protection Board of India (DPBI) as the central enforcement agency, the operational independence of the DPBI is subject to the direction of the Ministry of Electronics and Information Technology. This could affect perceptions of autonomy as the DPBI may engage in an investigative direction and compliance guidance but still be building efficiency against the EU model.

⁹ Digital Personal Data Protection Act 2023 vs. GDPR, JISA Softech, (june 13,2025)

¹⁰ GDPR Regulation (EU) 2016/679, art. 6; DPDP Act, 2023, sec 7 (India); Taxmann, DPDP Act vs. EU GDPR Compliance, (May 3, 2025).

In fact, both GDPR and DPDP create central regulatory authorities with oversight functions. However, while the supervisory Authorities under GDPR are to a very high degree autonomous with regard to law, they are backed by the EDPB for cross border consistency.

In addition the DPDPs data protection board is less decentralized and currently lacks a track of records of independent enforcement. Consequently, GDPR demonstrates a higher level of regulatory effectiveness, while DPDP relies on developing framework that aims to balance independence with administrative oversight.¹¹

3.2 Sanctions, Investigatory Powers and Incentives Mechanisms

The GDPR has strong enforcement mechanisms. Administrative fines of up to €20 million or 4% of worldwide annual turnover are given by the Supervisory Authorities depending on the gravity of violations. Other powers include ordering measures to correct the issue, suspension or prohibition of data processing, and imposing erasure of data. GDPR also mandates companies to have internal compliance measures, including data protection impact assessments, record-keeping, and reporting of breaches to the supervisory authority within 72 hours.

The DPDP Act similarly mandates penalties for non-compliance, although money penalties are lower compared to GDPR's. The Data Protection Board is able to inquire into complaints, issue directions to correct the violations, and impose compliance measures. DPDP organizations must also have grievance redressal mechanisms, perform risk-based analysis, and must provide transparency in data processing. Both pieces of legislation afford investigative and remedial powers, though GDPR's framework is more detailed and prescriptive than DPDP.

GDPR combines strong penalties with obligations and investigation powers, ensuring high level of accountability. The DPDP Act provides similar functions but with less fines, less granular enforcement procedures and more reliance on administrative guidance. Consequently, GDPR creates a stronger incentive for proactive, particularly during its implementation period.¹²

3.3 Efficiency in ensuring adherence to data protection obligations

GDPR's effectiveness in enforcement is based on its mature, decentralized design with robust legal powers, clearly articulated supervisory responsibilities, and large financial fines. The EDPB addresses uniform rule application across Member States, reducing regulatory holes and evasion. This system has typically resulted in good compliance, since organizations have robust incentives to adopt internal controls, such as data protection governance frameworks, training initiatives, and breach disclosure systems.

The DPDP Act is recently enacted, and its enforcement effectiveness is conditional on the DP Data Protection Board's organizational mechanisms, sufficient personnel, and independence of decision-making. Though the Act offers instruments like penalties, redressal of grievances, and audits for compliance, the actual-world efficiency in the same would be heavily reliant on the proactive monitoring by the Board and the timeliness in resolving complaints. Initial signs point toward emphasizing the balance of regulatory control against business and government operational requirements.

The enforcement mechanism of GDPR is more advanced and proven to be effective thanks to its decentralized architecture, substantial fines, and collaborative oversight. DPDP Act, on the other hand, is meant to develop a culture of compliance over time with room for adaptation in Indian situations. Although both act's approaches seek to safeguard data subjects' rights, GDPR upholds rigorous compliance, while DPDP adopts a balance between regulatory control and realistic enforceability in its initial implementation phase.¹³

4. Recommendations for Strengthening India's DPDP Act

4.1. Identifying gaps and challenges

Comparative examination of the DPDP Act and GDPR identifies various areas wherein the data protection regime of India can be bolstered. As opposed to GDPR, the DPDP Act does not have explicit provisions for sensitive personal data in favor of a uniform approach with reliance on the Significant Data Fiduciaries concept. This could curtail fine-grained protection for extremely sensitive types like health, biometric, or financial data. Also, whereas GDPR has a centralized and mature framework of autonomous Supervisory Authorities that work together through the EDPB, DPDP Act is based on a centralized Data Protection Board whose operational independence, funding, and enforcement record are still unfolding. The DPDP Act also offers fewer overt legal bases for data processing and less comprehensive direction on matters of accountability measures like data protection impact assessments, obligatory record-keeping, and designation of Data Protection Officers, which are compulsory under GDPR. Lastly, DPDP penalties are lower and compliance processes less stipulative, possibly lessening the incentive for active conformity to data protection requirements.

4.2 Suggested improvements and best practices

India's framework needs a lot more enhancement in line with the world. The following are some measures:

First, creating a tiered, sensitive personal data categorization collection with more stringent restrictions on processing would improve individual entitlement protection.

¹¹GDPR Regulation (EU) 2016/679, arts. 51-57; DPDP Act, 2023, sec 30-34 (India); KSANDK, DPDP Act vs GDPR & Global Privacy Laws, (Sept. 22, 2025).

¹² Regulation (EU) 2016/679, arts. 83, 84; DPDP Act, 2023, Sec 36-39 (India).

¹³ Latham & Watkins LLP, India's Digital Personal Data Protection Act 2023 vs. the GDPR, (2025).

Second, it should be established by law that the "independence" of the data protection board is further supported by sufficient provisions of human resources and open accountability measures for greater oversight and enforcement.

Thirdly, prescriptive compliance requirement coverage could be increased, for instance, mandatory DPIAs very robust internal audit mechanism apart from the appointment of data protection officers for critical data fiduciaries, which would drive proactive governance of data.

Fourthly, strengthening penalties for non-compliance with explicit remedial powers would seriously enhance deterrents and improve the efficacy of enforcement.

Finally, adopting some of the best practices in GDPR, such as detailed guidance on cross-border data transfers, accountability, transparency and individual rights, will ensure India build a global edge towards interoperability and trust in data protection.

5. Conclusion

It carries out extensive comparative research between the General Data Protection Regulation (GDPR) of the European Union and the Digital Personal Data Protection (DPDP) Act, 2023 of India. The first milestone is for data protection, where an individual becomes an important party with respect to his/her personal data, imposing obligations on parties dealing with such data. Indeed, the DPDP Act is a major step in creating a data protection mechanism tailored to the specific socio-economic and technological context in which India operates, while the GDPR is lauded as a truly global benchmark in privacy legislation.

These rights included in GDPR are some of the most extensive and exhaustive rights available to individuals including, the right to access, rectification, erasure, data portability, and not being subjected to automated decision-making. They come along with stringent obligations on data controllers and processors, backed up by an enforceable scheme, decentralized supervisory authorities, and enormous penalties, unlike the DPDP Act, which is based on a much simpler framework focusing on digital personal data through a consent-based approach, practical rights like correction, withdrawal of consent, and grievance redressal. The DPDP Act brings in broader exemptions for the government and proportionately less severe penalties, which appears to be an Indian way of balancing privacy with digital economic growth and regulatory feasibility.

Despite the differences, significant commonalities in principles such as consent, extraterritoriality, fiduciary accountability, and right to informational self-determination do exist. However, there are still challenges for the DPDP Act in areas of independence of enforcement, protection of sensitive data in a broader context, and efficacy in implementation.

To be in line with the spirit of global best practices, India would require strengthening regulatory independence, improved penalty regimes, distinction and classification of sensitive data, and the extension of the scope of individual rights. Therefore, the DPDP Act has made India a sovereignty-based consent-first model on the global canvas of emerging data protection and possible models for developing economies in drafting balanced privacy laws.

6. References

1. Pameela George Puthenveeti (2024) - "DPDPA 2023 vs. GDPR: A Comparative Analysis of India's & EU's Data Privacy Law." : <https://lawandtech.ie/dpdpa-2023-vs-gdpr-a-comparative-analysis-of-indias-eus-data-privacy-laws/>
2. Hemalatha G. and Saikrupaa K. (2023) - Comparative analysis of GDPR and Digital Personal Data Protection Act, 2023. : <https://www.ijllr.com/>
3. Bhargav Chaganti (2024) - The Right to be Forgotten: A Comparative Analysis of the GDPR and the DPDPA. : <https://ijllr.com/>
4. Vaibhav Dharod and Kevin Tauro (2023) - Assessing India's Digital Personal Data Protection Act, 2023: A Comparative Study with GDPR. : <https://ijllr.com/>
5. Prabhash Dalei (2025) - The Digital Personal Data Protection Act, 2023: A Legal Analysis in Light of Global Data Protection Standards. : <https://www.lawjournals.org/>
6. "Comparative Analysis of GDPR and Digital Personal Data Protection Act, 2023" by Hemalatha G and Saikrupaa K (Indian Journal of Creative Research Thoughts : <https://www.ijcrt.org/papers/IJCRT2312087.pdf>
7. "The Digital Personal Data Protection Act, 2023: A Legal Analysis in Light of Global Data Protection Standards" by Prabhash Dalei (International Journal of Law, 2025) : <https://www.lawjournals.org/assets/archives/2025/vol11issue3/11064.pdf>
8. "India's Digital Personal Data Protection Act 2023 vs. the GDPR: A Comparison" (Law Firm Publication) : <https://www.lw.com/admin/upload/SiteAttachments/Indias-Digital-Personal-Data-Protection-Act-2023-vs-the-GDPR-A-Comparison.pdf>
9. "Comparison Between GDPR and India's Digital Personal Data Protection Act" (Indian Journal of Law, 2025): <https://law.shodhsagar.com/index.php/j/article/view/85>
10. "Critical Analysis Of The Digital Personal Data Protection Act 2023" (Indian Journal of Law and Legal Research) : <https://www.ijllr.com/post/critical-analysis-of-the-digital-personal-data-protection-act-2023>
11. "DPDPA 2023 vs. GDPR: A Comparative Analysis of India's & EU's Data Privacy Laws" – EmildAI : <https://emildai.eu/dpdpa-2023-vs-gdpr-a-comparative-analysis-of-indias-eus-data-privacy-laws/>

-
12. "The Indian Digital Personal Data Protection Act, 2023: An Early Overview" by D Korff :
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4614984/