IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

COMPARATIVE ANALYSIS OF GDPR AND DIGITAL PERSONAL DATA PROTECTION ACT, 2023.

[1]Hemalatha G, [2]Saikrupaa K

[1] Final Year BBA LL.B. (Hons), [2]Final Year B.com LL.B. (Hons)

[1]School of Law, Sastra University, Thanjavur, Tamil Nadu, India., [2]School of Law, Sastra University, Thanjavur, Tamil Nadu, India.

Abstract:

In order to ensure the protection of individuals' personal data in the digital age, it is essential to have a well-defined set of data protection regulations in place. This article provides a comparison of two of the most important data protection regulations in India, namely the GDPR and the DPDP. The Digital Personal Data Protection Act (DPDPA) is a major development for India's Privacy System, as it aims to replace the existing patchwork of data protection laws and regulations. There has been a long-standing need for the Government of India to establish a comprehensive and unified data protection regime that is comparable to global standards. Because of its identical norms and regulations, the Digital Personal Data Protection Act is deemed equivalent to the General Data Protection Regulation. The first section outlines the measures that led to the creation of GDPR and how they have influenced the creation of the Digital Personal Data Protection Act. This article provides an overview while comparing and discussing how DPDP compares to the EU's GDPR. GDPR has a significant impact on the development of the DPDPA, 2023. While both legislations seek to protect personal data, they differ in a number of ways, including scope, territorial applicability, and data subject rights. Furthermore, we want to delve deeper into the key clauses of both India's Personal Data Protection Act and the EU's GDPR. We have also tried to highlight certain key issues and analysis that are present in the newly formed Digital Personal Data Protection Act, 2023.

Index Terms- The General Data Protection Regulation, Digital Personal Data Protection Act, Personal Data, Data Subject Rights, Consent, Privacy, Similarities and Key differences.

i. Introduction:

The Digital Revolution has brought a vast increase in the collection, processing, and utilization of personal data. Consequently, the need for robust data protection laws have become paramount to safeguard individual's privacy and ensure responsible data handling practices. The General data Protection Regulation (GDPR), enforced in the European Union (EU) in 2018, is a landmark piece of legislation in the field of data protection. The General Data Protection Regulation (GDPR) stands as one of the most significant milestones and a revolutionary step in global data protection and privacy regulation. GDPR has redefined the way organizations collect, process and protect personal data within European Union (EU). It has been hailed as a significant milestone in data protection legislation. The Digital Personal Data Protection Act, 2023 (DPDPA 2023) is a landmark piece of legislation enacted by the Indian government which concerns itself to the processing of digital personal data in a manner that recognises both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes. This article aims to compare these two regulations, identify their similarities and differences, and address the research gaps in the existing literature.

ii. Scope and Applicability:

According to section 3[1], The GDPR applies to all EU member states and any organization processing personal data of EU residents, regardless of the organization's location. According to Section 3[2], The scope of the DPDP Act extends to the processing of digital personal data within India where such data is: (i) collected online, or (ii) collected offline and is made in a digital form subsequently. It will also apply to the processing of personal data outside India if it is for offering goods or services in India.

According to section 3(c)(i)[3] The act does not apply to personal data processed by an individual for any personal or domestic purpose; (ii) personal data that is made publicly available by— (A) the Data Principal to whom such personal data relates or (B) any other person who is under an obligation to make such personal data publicly available.

iii. GDPR- Significance & Key Principles:

- GDPR grants individuals' greater control over their personal data. It encourages or organizations to collect and process only the data that is necessary for a specific purpose. This principle promotes responsible data handling and minimises the risk of data breaches.
- GDPR mandates clear and informed consent for data processing. Organizations must explain how they use data in plain language. This enhances transparency and ensures individuals are aware of what happens with their data.
- It imposes stringent requirements on data security, including data encryption, breach notification, and data protection impact assessments. These measures help safeguard data against breaches and cyber threats.
- GDPR's reach extends beyond the EU. Any organization processing the data of EU residents must comply, regardless of their location. This has global implication. Promoting companies worldwide to adopt similar data protection measures. This means that companies based outside the EU, but that offer goods or services to individuals within the EU or monitor their behaviour, are subject to the GDPR.
- GDPR has driven efforts to harmonize data protection laws across regions and countries. It serves as a model for other nations looking to strengthen the data protection regulations.
- GDPR introduced hefty fines for non-compliance, which can reach up to 20 million Euros or 4% of a company's global annual turnover, whichever is higher. This financial risk has incentivized organizations to take data protection seriously. This has motivated organizations around the world to take data protection seriously and ensure compliance with GDPR requirements.
- GDPR has raised awareness about the importance of data privacy. People are more conscious about their data rights, and organizations are more diligent in protecting sensitive information.
- Compliance with GDPR can enhance an organization's reputation and customer trust. It also encourages data-driven innovation by promoting responsible data management.
- One of the key principles of the GDPR is that personal data can only be transferred to countries outside the EU if those countries provide an adequate level of data protection. This means that the EU considers the data protection laws and practices of these countries to be equivalent to the protection offered within the EU.
- The European Commission maintains a list of countries that have been deemed to provide adequate protection. For countries that are not on the adequacy list, organizations can still transfer personal data outside the EU if they implement appropriate safeguards. These safeguards may include using standard contractual clauses approved by the European Commission, implementing binding corporate rules within a multinational organization, or relying on approved codes of conduct or certification mechanisms.

[1] The General Data Protection Regulation 2018, https://gdpr-info.eu/art-3-gdpr/
[2] Section 3, The Digital Personal Data Protection Act, 2023
https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf
[3] Section 3(c)(i) of The Digital Personal Data Protection Act, 2023

- In addition to adequacy decisions and appropriate safeguards, organizations can also rely on derogations under the GDPR to transfer personal data outside the EU. These derogations include obtaining explicit consent from the individuals whose data is being transferred, ensuring the transfer is necessary for the performance of a contract with the individual, or protecting vital interests of the individual.

- In summary, the GDPR has a significant impact on international data protection. It requires organizations outside the EU to comply with its provisions if they process the personal data of individuals within the EU. The GDPR establishes mechanisms, such as adequacy decisions, appropriate safeguards, and derogations, to facilitate the transfer of personal data outside the EU while ensuring an adequate level of protection. Compliance with the GDPR is crucial for organizations to maintain access to the EU market and avoid substantial financial penalties.

iv. SALIENT FEATURES OF THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023.

HIGHLIGHTS OF THE ACT

Personal data is classified as an information which relates an individual human being who can be identified in relation to that data. Businesses as well as government entities process personal data for the purpose of delivering of goods and services. Processing of personal data gives an understanding of the individual's preferences, which may be useful for customisation, targeted advertising, and developing recommendations. Processing of personal data may also help for enforcement of certain laws, rules and regulations. Unchecked processing may have adverse implications for the privacy of individuals, which has been recognised as a fundamental right[4]. It may subject individuals to harm such as financial loss, loss of reputation, and profiling.

Use of personal data is regulated under the Information Technology (IT) Act, 2000[5]. In 2017, the central government constituted a Committee of Experts on Data Protection, chaired by Justice B. N. Srikrishna, to examine issues relating to data protection in the country. The Committee submitted its report in July 2018[6]. Based on the recommendations of the Committee, the Personal Data Protection Act, 2019 was introduced in Lok Sabha in December 2019[7]. The Act was referred to a Joint Parliamentary Committee which submitted its report in December 2021. In August 2022, the Act was withdrawn from Parliament. In November 2022, a Draft Act was released for public consultation[8]. In August 2023, the Digital Personal Data Protection Act, 2023 was introduced in India by the Parliament[9].

v. Key Features

- **Applicability:** The Act applies to the processing of digital personal data within India where such data is: (i) collected online, or (ii) collected offline and is digitised. It will also apply to the processing of personal data outside India if it is for offering goods or services in India. Personal data is defined as any data about an individual who is identifiable by or in relation to such data. Processing has been defined as wholly or partially automated operation or set of operations performed on digital personal data. It includes collection, storage, use, and sharing.

- **Consent:** Personal data may be processed only for a lawful purpose after obtaining the consent of the individual. A notice must be given before seeking consent. The notice should contain details about the personal data to be collected and the purpose of processing. Consent may be withdrawn at any point in time. Consent will not be required for 'legitimate uses' including: (i) specified purpose for which data has been provided by an individual voluntarily, (ii) provision of benefit or service by the

[4] [1]. Justice K.S. Puttaswamy (Retd) vs. Union of India, W.P. (Civil) No 494 of 2012, Supreme Court of India, August 24, 2017.
[5] Report of the Joint Committee on the Personal Data Protection Act, 2019, December 2021., The Information Technology Act, 2000.
[6] 'A Free and Fair Digital Economy Protecting Privacy, Empowering Indians', Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, July 2018.
[7] The Personal Data Protection Act, 2019, as introduced in Lok Sabha.
[8] The Draft Digital Personal Data Protection Act, 2022, Ministry of Electronics and Information Technology, November 18, 2022.
[9] The Digital Personal Data Protection Act, 2019, as introduced in Lok Sabha.

government, (iii) medical emergency, and (iv) employment. For individuals below 18 years of age, consent will be provided by the parent or the legal guardian.

- **Rights and duties of data principal:** An individual whose data is being processed (data principal), will have the right to: (i) obtain information about processing, (ii) seek correction and erasure of personal data, (iii) nominate another person to exercise rights in the event of death or incapacity, and (iv) grievance redressal. Data principals will have certain duties. They must not: (i) register a false or frivolous complaint, and (ii) furnish any false particulars or impersonate another person in specified cases. Violation of duties will be punishable with a penalty of up to Rs 10,000.

- **Obligations of data fiduciaries:** The entity determining the purpose and means of processing, (data fiduciary), must: (i) make reasonable efforts to ensure the accuracy and completeness of data, (ii) build reasonable security safeguards to prevent a data breach, (iii) inform the Data Protection Board of India and affected persons in the event of a breach, and (iv) erase personal data as soon as the purpose has been met and retention is not necessary for legal purposes (storage limitation). In case of government entities, storage limitation and the right of the data principal to erasure will not apply.

- **Transfer of personal data outside India:** The Act allows transfer of personal data outside India, except to countries restricted by the central government through notification.

- **Exemptions:** Rights of the data principal and obligations of data fiduciaries (except data security) will not apply in specified cases. These include: (i) prevention and investigation of offences, and (ii) enforcement of legal rights or claims. The central government may, by notification, exempt certain activities from the application of the Act. These include: (i) processing by government entities in the interest of the security of the state and public order, and (ii) research, archiving, or statistical purposes.

- **Data Protection Board of India:** The central government will establish the Data Protection Board of India. Key functions of the Board include: (i) monitoring compliance and imposing penalties, (ii) directing data fiduciaries to take necessary measures in the event of a data breach, and (iii) hearing grievances made by affected persons. Board members will be appointed for two years and will be eligible for re-appointment. The central government will prescribe details such as the number of members of the Board and the selection process. Appeals against the decisions of the Board will lie with TDSAT.

- **Penalties:** The schedule to the Act specifies penalties for various offences such as up to: (i) Rs 200 crore for non-fulfilment of obligations for children, and (ii) Rs 250 crore for failure to take security measures to prevent data breaches. Penalties will be imposed by the Board after conducting an inquiry.

vi. KEY ISSUES AND ANALYSIS

Exemptions to the State may have adverse implications for privacy

Personal data processing by the State has been given several exemptions under the Act. As per Article 12 of the Constitution, the State includes: (i) central government, (ii) state government, (iii) local bodies, and (iv) authorities and companies set up by the government. There may be certain issues with such exemptions.

The Act may enable unchecked data processing by the State, which may violate the right to privacy:

The Supreme Court (2017) has held that any infringement of the right to privacy should be proportionate to the need for such interference. Exemptions for the State may lead to data collection, processing, and retention beyond what is necessary. This may not be proportionate, and may violate the fundamental right to privacy[10].

The Act empowers the central government to exempt processing by government agencies from any or all provisions, in the interest of aims such as the security of the state and maintenance of public order. None of the rights of data principals and obligations of data fiduciaries (except data security) will apply in certain cases such as processing for prevention, investigation, and prosecution of offences. The Act does not require

[10] Justice K.S. Puttaswamy (Retd) vs. Union of India, W.P. (Civil) No 494 of 2012, Supreme Court of India, August 24, 2017.

government agencies to delete personal data, after the purpose for processing has been met. Using the above exemptions, on the ground of national security, a government agency may collect data about citizens to create a 360-degree profile for surveillance. It may utilise data retained by various government agencies for this purpose. This raises the question whether these exemptions will meet the proportionality test.

For interception of communication on grounds such as national security, the Supreme Court (1996) had mandated various safeguards including: (i) establishing necessity, (ii) purpose limitation, and (iii) storage limitation[11]. These are similar to the obligations of data fiduciaries under the Act, the application of which has been exempted. The Srikrishna Committee (2018) had recommended that in case of processing on grounds such as national security and prevention and prosecution of offences, obligations other than fair and reasonable processing and security safeguards should not apply. It observed that obligations such as storage limitation and purpose specification, if applicable, would be implemented through a separate law. India does not have any such legal framework.

In the United Kingdom, the data protection law enacted in 2018, provides similar exemptions for national security and defence[12]. However, actions such as bulk processing of personal datasets by government agencies for intelligence and law enforcement activities are regulated under the Investigatory Powers Act, 2016[13]. A warrant for such action is issued by the Secretary of State (i.e., Home Minister), which requires prior approval by a Judicial Commissioner. Necessity and proportionality for such actions must be established. Data retention beyond the period of warrant is restricted. This law also provides for parliamentary oversight.

Whether overriding consent for purposes such as benefit, subsidy, license, and certificates is appropriate:

The Act overrides consent of an individual where the State processes personal data for provision of benefit, service, license, permit, or certificate. It specifically allows use of data processed for one of these purposes for another. It also allows use of personal data already available with the State for any of these purposes. Hence, it removes purpose limitation, which is one of the key principles for protection of privacy. Purpose limitation means data should be collected for specific purposes, and should be used only for that purpose. The question is whether such exemptions are appropriate.

Since data taken for various purposes could be combined, this could allow profiling of citizens. On the other hand, if consent were required, individuals would have the autonomy and control over collection and sharing of their personal data.

The Act does not regulate harm arising from processing of personal data

The Act does not regulate risks of harms arising out of processing of personal data. The Srikrishna Committee (2018) had observed that harm is a possible consequence of personal data processing. Harm may include material losses such as financial loss and loss of access to benefits or services. It may also include identity theft, loss of reputation, discrimination, and unreasonable surveillance and profiling. It had recommended that harms should be regulated under a data protection law.

The Personal Data Protection Act, 2019 had defined harm to include: (i) mental injury, (ii) identity theft, (iii) financial loss, (iv) reputational loss, (v) discriminatory treatment, and (vi) observation or surveillance not reasonably expected by the data principal[14]. The 2019 Act required data fiduciaries to take measures to prevent, minimise, and mitigate risks of harm. These included undertaking evaluation of these risks in impact assessments and audits. It also granted the data principal the right to seek compensation from data fiduciary or data processor, where the data principal has suffered harm. The Joint Parliamentary Committee, examining the 2019 Act, had recommended retaining the provisions regarding harm arising from processing of personal data.

---

[11] Rule 419A, The Indian Telegraph Rules, 1951 issued under Section 7 (2) of the Indian Telegraph Act, 1885., People's Union for Civil Liberties (PUCL) vs Union of India, Supreme Court of India, December 18, 1996.

[12] Chapter 3, Data Protection Act, 2018, United Kingdom.

[13] Part 6, 7, and 8, Investigatory Powers Act, 2016, United Kingdom.

[14] Clause 2 (20), Clause 2 (38), Clause 15, The Personal Data Protection Act, 2019, as introduced in Lok Sabha.

General Data Protection Regulation (GDPR) of the European Union also regulates risks of harm and provides for compensation to the data principal in the event of harm[15].

Right to data portability and the right to be forgotten not provided:

The Act does not provide for the right to data portability and the right to be forgotten. The 2018 Draft Act and the 2019 Act introduced in Parliament provided for these rights[16]. The Joint Parliamentary Committee, examining the 2019 Act, recommended retaining these rights. GDPR also recognises these rights[17]. The Srikrishna Committee (2018) observed that a strong set of rights of data principals is an essential component of a data protection law. These rights are based on principles of autonomy, transparency, and accountability to give individuals control over their data.

Adequacy of protection in case of cross-border transfer of data

The Act provides that the central government may restrict the transfer of personal data to certain countries through a notification. This implies the transfer of personal data to all other countries without any explicit restrictions. This question is whether this mechanism will provide adequate protection.

The aim of the regulation of transfer of personal data outside India is to safeguard the privacy of Indian citizens. In the absence of robust data protection laws in another country, data stored there may be more vulnerable to breaches or unauthorised sharing with foreign governments as well as private entities. The 2019 Act required that for certain categories of data, transfer to a country should be allowed only if it provides for adequate level of protection[18]. The 2022 Draft Act took a different approach, with the central government notifying countries where any personal data may be transferred[19]. Both these mechanisms require a case-by-case evaluation of the standards in every country to which data may be transferred. The mechanism to restrict countries selectively does not require such exhaustive evaluation.

Shorter appointment term may impact independence of the Board

The Act provides that members of the Data Protection Board of India will function as an independent body. Members will be appointed for two years and will be eligible for re-appointment. A short term with the scope for re-appointment may affect independent functioning of the Board.

Key functions of the Board are monitoring compliance, carrying out investigations, and adjudging penalties. In case of Tribunals, the Supreme Court (2019) had observed that short-term along with the provisions of re-appointment increases influence and control of the Executive[20]. Regulatory authorities with adjudicatory role such as the Central Electricity Regulatory Commission and the Competition Commission of India have a term of five years under respective Acts[21]. In case of TRAI, the term of appointment is three years[22]. The term of appointment to SEBI is five years, specified through Rules.[25]

Exemption from notice for consent may not be appropriate

The Act empowers the central government to notify certain data fiduciaries or classes of data fiduciaries including startups from certain obligations. This must be done with due regard to volume and nature of personal data. One of the obligations which may be exempted is notice for consent. The requirement to seek free and informed consent will continue to apply in case of these entities. However, if there is no obligation to provide notice regarding nature of data collected and purpose of processing, it may be argued that a data principal will not be able to provide informed consent.

[15] Recital 75, Article 82, General Data Protection Regulation of European Union.
[16] Clause 19, The Personal Data Protection Bill, 2019, as introduced in Lok Sabha.
[17] Article 20, General Data Protection Regulation, European Union.
[18] Clause 33 and 34, The Personal Data Protection Bill, 2019, as introduced in Lok Sabha.
[19] Clause 17, The Draft Digital Personal Data Protection Bill, 2022, Ministry of Electronics and Information Technology, November 18, 2022.
[20] Rojer Mathew versus South Indian Bank Ltd & Ors., 2019 (369) ELT3 (S.C.), Supreme Court of India, November 13, 2019.
[21] Section 10 (1), The Competition Act, 2002.
[22] Section 5 (2), The Telecom Regulatory Authority of India Act, 1997.

vii. Comparative Analysis of GDPR and DPDPA, 2023:

Definition of Personal Data:

GDPR: GDPR provides a broad definition of personal data, which includes any information that can directly or indirectly identify an individual.

Section 2(t) of the Digital Personal Data Protection Act, 2023, personal data means any data about an individual who is identifiable by or in relation to such data.

Data Subject Rights:

Both the regulations provide individuals with certain rights regarding their personal data.

GDPR: The GDPR grants several rights to data subjects, including the right to access their personal data, the right to rectify inaccurate data, the right to erasure (also known as the right to be forgotten), the right to data portability, and the right to object to data processing.

Digital Personal Data Protection Act, 2023: The Digital Personal Data Protection Act, 2023 recognizes similar data subject rights, but it is limited when compared to those offered under the GDPR. This act guarantees a right of access and a right to erasure and correction, in addition to a right to receive notice before consent, and the right not to be subject to solely automated decision making are missing.

Consent and Lawful Basis for Processing:

GDPR: GDPR emphasizes the importance of obtaining valid consent from data subjects for processing their personal data. It sets a high standard for consent by requiring it to be freely given, specific, informed, and unambiguous. The regulation also provides other lawful bases for processing personal data, such as the necessity of processing for the performance of a contract or compliance with legal obligations.

Digital Personal Data Protection Act, 2023: The Digital Personal Data Protection Act, 2023 Consent of the data principal is one of the foundational principles, using which data fiduciary data controller may process personal data. Broadly speaking, the basic principles of consent are similar under DPDP and the GDPR i.e. consent should be free, specific and informed. Further, both GDPR and DPDP require a legitimate reason (purpose) to process personal data. Another common provision under both GDPR and DPDP requires the data fiduciary to demonstrate that consent has been obtained in compliance with the respective legislations. DPDP imposes additional obligations in relation to accessibility by requiring the consent request to be provided in several languages at the option of the data principal.

Data Breach Notification:

GDPR: GDPR mandates organizations to report personal data breaches to the relevant supervisory authority within 72 hours of becoming aware of the breach. In certain cases, data subjects may also need to be notified if the breach is likely to result in high risks to their rights and freedoms.

Digital Personal Data Protection Act, 2023: The DPDP mandates the data fiduciary to notify the Data Protection Board and each affected data principal, in the event of any personal data breach. Unlike the DPDP, an obligation to inform the data subject of a breach is triggered under the GDPR only when there is high risk to the impacted individuals.

Data Protection Officer (DPO):

GDPR: GDPR requires certain organizations to appoint a Data Protection Officer (DPO) if their core activities involve regular and systematic monitoring of data subjects on a large scale or if they process sensitive personal data on a large scale.

Digital Personal Data Protection Act, 2023: "Data Protection Officer" means an individual appointed by the Significant Data Fiduciary under clause (a) of sub-section (2) of section 10; A significant data fiduciary may appoint the data protection officer and such officer shall represent the data fiduciary for the purposes of this act. He is responsible to the Board of Directors or similar governing body of the Significant Data Fiduciary and be the point of contact for the grievance redressal mechanism.

viii. Conclusion:

The Author emphasizes the evolving international approach to data protection laws and the importance of understanding these trends for policymakers, organizations, and individuals. The GDPR and the DPDPA are significant data protection regulations with similarities and differences. Strengthening data protection laws and addressing key issues in data protection are crucial in the digital age. The data protection laws and regulations are evolving in response to the changing digital landscape. Strengthening data protection laws, the emergence of data localization requirements, and the focus on technological solutions are some of the key trends that will shape the future of data protection globally. Understanding these trends and their implications is crucial we continue to navigate the complex landscape of data privacy and security in the years to come.

ix. References:

1. EUDeligation (2017). EU-U.S. Privacy Shield. Retrieved from https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-privacy-shield_en

2. ersheds (2017). EU GDPR – Cross-Border Data Transfers. Retrieved from https://www.eversheds-sutherland.com/global/en/what/articles/index.page

3. Organization for Economic Cooperation and Development (2018). APEC Cross-Border Privacy Rules. Retrieved from https://www.oecd.org/sti/ieconomy/cross-border-privacy-rules.htm