Volume 32, May 2024 ISSN 2581-5504

"Comparative Analysis of the Digital Personal Data Protection Act of India 2023 and GDPR"

***Mehreen Imtiaz**
Amity Law School
Uttar Pradesh

****Dr. Deepika Prakash**
Amity Law School
Uttar Pradesh

Abstract

This article aims to provide a comparative analysis of two crucial data protection regulations in India, namely the GDPR and the DPDP. The Digital Personal Data Protection Act (DPDPA) represents a significant milestone in India's privacy framework, seeking to replace the existing array of data protection laws and regulations with a unified and comprehensive regime.

Given its alignment with global standards, the Digital Personal Data Protection Act is considered equivalent to the General Data Protection Regulation (GDPR). The article begins by discussing the factors that led to the development of the GDPR and how they influenced the creation of the Digital Personal Data Protection Act. It provides an overview of both regulations and compares them, highlighting differences in scope, territorial applicability, and data subject rights.

Overall, the article seeks to provide a comprehensive understanding of the similarities and differences between the GDPR and the DPDP, offering insights into their respective frameworks and implications for data protection in India.

Introduction

The introduction of the Digital Personal Data Protection Act of India 2023 (DPDP) marks a significant milestone in India's data protection landscape. With the rapid digitization of society and the proliferation of data-driven technologies, there has been a growing recognition of the need to enact comprehensive legislation to safeguard individuals' personal data.
By conducting a thorough comparison of these two regulatory frameworks, this analysis aims to provide insights into how the DPDP aligns with international best practices and how it may impact businesses, individuals, and data protection practices in India. Additionally, it will highlight areas where the DPDP may diverge from the GDPR and the rationale behind such differences. Overall, this analysis aims to contribute to a better understanding of the evolving data protection landscape in India and its implications for stakeholders in the digital age.

Overall, both the GDPR and the DPDPA 2023 represent significant advancements in data protection legislation, signaling a global shift towards stronger protections for individuals' personal data in the digital age. As countries around the world continue to grapple with the challenges posed by digitalization, robust data protection laws like the GDPR and the DPDPA

Volume 32, May 2024 ISSN 2581-5504

2023 play a crucial role in safeguarding privacy rights and promoting trust in digital services and platforms.

Comparative analysis of GDPR and DPDPA, 2023

The Comparative Analysis of GDPR and DPDPA, 2023 aims to provide an in-depth examination of the key similarities and differences between the General Data Protection Regulation (GDPR) enacted by the European Union and the Digital Personal Data Protection Act, 2023 (DPDPA 2023) enacted by India. This analysis will focus on several key areas, including scope, principles, data subject rights, compliance requirements, cross-border data transfers, regulatory enforcement mechanisms, and penalties for non-compliance. By comparing and contrasting these two data protection regulations, the analysis seeks to identify best practices, challenges, and opportunities for organizations operating in India and the European Union to ensure compliance with data protection laws and protect individuals' privacy rights in the digital age. Through this comparative analysis, stakeholders will gain valuable insights into the evolving landscape of data protection regulation and the implications for global data governance and privacy management practices

Literature Review

A literature review provides insights into the similarities, differences, and implications of these regulations:

Scope and Applicability: Several studies have examined the scope and territorial applicability of the DPDPA 2023 and GDPR. Researchers have analyzed how the regulations define personal data, data controllers, and data processors, and their implications for organizations operating across borders.

Data Subject Rights: Scholars have explored the data subject rights conferred by the DPDPA 2023 and GDPR, such as the right to access, rectify, erase, and restrict processing of personal data. Comparative studies have evaluated the effectiveness of these rights in empowering individuals to control their personal data.

Data Protection Principles: The literature has delved into the underlying data protection principles of both regulations and their alignment with international best practices. Researchers have examined how the principles of lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, and confidentiality are implemented in practice.

Data Breach Notification: Studies have assessed the data breach notification requirements under the DPDPA 2023 and GDPR, including the thresholds, timelines, and obligations for organizations to report breaches to supervisory authorities and affected individuals. Comparative analyses have highlighted the differences in breach notification practices and their impact on organizational risk management.

Cross-Border Data Transfers: Scholars have investigated the mechanisms and challenges associated with cross-border data transfers under the DPDPA 2023 and GDPR. Comparative

Volume 32, May 2024 ISSN 2581-5504

studies have examined the adequacy decisions, standard contractual clauses, binding corporate rules, and other transfer mechanisms available to organizations for lawful international data transfers.

Regulatory Enforcement and Penalties: The literature has explored the enforcement mechanisms and penalties for non-compliance with the DPDPA 2023 and GDPR. Researchers have analyzed the roles and powers of supervisory authorities, investigative procedures, administrative fines, and other sanctions imposed on violators, as well as their effectiveness in promoting compliance.

Data Localization Requirements: Studies have examined the data localization requirements introduced by the DPDPA 2023 and their implications for data sovereignty, security, and economic development. Comparative analyses have assessed the impact of data localization on multinational organizations' data management practices and infrastructure investments.

Overall, the literature review provides valuable insights into the comparative analysis of the DPDPA 2023 and GDPR, highlighting their key provisions, implications, and challenges for organizations, policymakers, and stakeholders in India and the European Union.

Objective

1. The comparative analysis is to identify and analyze the key similarities and differences between the Digital Personal Data Protection Act of India 2023 (DPDPA 2023) and the General Data Protection Regulation (GDPR).

2. To understand the implications of the DPDPA 2023 and GDPR for data protection practices, privacy rights, and organizational responsibilities.

3. By comparing the DPDPA 2023 and GDPR, the analysis seeks to identify best practices in data protection regulation and areas for improvement.

DPDPA vs GDPR – comparative analysis of understanding the lawfulness of processing

The GDPR outlines six lawful bases for processing personal data:

Consent: Processing is lawful if the data subject has given consent to the processing of their personal data for specific purposes.

Contractual necessity: Processing is necessary for the performance of a contract with the data subject or for taking pre-contractual steps at the data subject's request.

Legal obligation: Processing is necessary for compliance with a legal obligation to which the data controller is subject.Vital interests: Processing is necessary to protect the vital interests of the data subject or another natural person.

Public task: Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller.

Volume 32, May 2024 ISSN 2581-5504

Legitimate interests: Processing is necessary for the legitimate interests pursued by the data controller or a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject.

DPDPA:

While the specifics of the DPDPA are not available, it is expected to alig with international standards such as the GDPR in determining the lawfulness of processing personal data.

It is likely to include similar lawful bases for processing, such as consent, contractual necessity, legal obligation, vital interests, public task, and legitimate interests.

The DPDPA may also introduce additional provisions or considerations relevant to the Indian context.

Comparative Analysis:

Both the GDPR and the DPDPA emphasize the importance of establishing a lawful basis for processing personal data.

Both regulations recognize consent as one of the lawful bases for processing, but they also allow for other legal grounds depending on the specific circumstances.

The GDPR's emphasis on data subject rights and principles such as transparency and purpose limitation influence how the lawfulness of processing is interpreted and applied.

While the specifics of the DPDPA are yet to be finalized, it is expected to share similarities with the GDPR in terms of the lawful bases for processing and the principles of data protection.

In summary, the GDPR and the DPDPA are likely to have comparable frameworks for determining the lawfulness of processing personal data, with both regulations emphasizing the need for transparency, fairness, and respect for individuals' rights.

Key issues and analysis digital personal data protection act of INDIA 2023 and GDPR

Scope and Applicability: One of the key differences between the Digital Personal Data Protection Act of India 2023 (DPDPA 2023) and the General Data Protection Regulation (GDPR) is their scope and territorial applicability. While the GDPR applies to the processing of personal data of individuals within the European Union (EU) and the European Economic Area (EEA), the DPDPA 2023 applies to the processing of digital personal data within India. This difference in scope may impact multinational organizations operating in both jurisdictions.

Data Subject Rights: Both the DPDPA 2023 and GDPR confer certain rights upon data subjects regarding their personal data. These rights include the right to access, rectify, erase, restrict processing, and data portability. However, there may be variations in the implementation and enforcement of these rights, as well as differences in the procedures for data subject requests between the two regulations.

Volume 32, May 2024 ISSN 2581-5504

Data Breach Notification: Both the DPDPA 2023 and GDPR impose obligations on organizations to notify supervisory authorities and affected individuals in the event of a personal data breach. However, there may be differences in the thresholds, timelines, and requirements for data breach notification between the two regulations, leading to complexities for multinational organizations in managing data breaches across jurisdictions.

Regulatory Enforcement and Penalties: The enforcement mechanisms and penalties for non-compliance with the DPDPA 2023 and GDPR may vary. While both regulations empower supervisory authorities to investigate and impose administrative fines for violations, the specific enforcement practices and penalty regimes may differ between India and the EU. This could impact the risk assessment and compliance strategies of organizations operating in both jurisdictions.

In conclusion, while the DPDPA 2023 and GDPR share common objectives of protecting personal data and enhancing privacy rights, there are key differences in their scope, requirements, and enforcement mechanisms. Organizations operating in India and the EU need to carefully analyze these differences and tailor their compliance strategies accordingly to ensure alignment with both regulations

Seven (7) such areas of difference among the GDPR and DPDP:

Seven key areas of difference between the GDPR (General Data Protection Regulation) and the Indian Data Protection and Privacy Bill (DPDP):

Scope and Jurisdiction:

GDPR: Applies to all organizations processing personal data of individuals within the European Union, regardless of the organization's location.

DPDP: Likely applies to entities processing personal data within India, with provisions for extraterritorial applicability under certain conditions, but primarily focused on data processed within Indian borders.

Data Localization:

GDPR: Does not mandate data localization but imposes restrictions on transferring personal data outside the European Economic Area (EEA) without adequate safeguards.

DPDP: May include provisions for data localization, requiring certain categories of sensitive personal data to be stored and processed within India.

Data Subject Rights:

GDPR: Grants individuals rights such as the right to access, rectification, erasure, restriction of processing, data portability, and objection to processing.

DPDP: Expected to include similar rights for individuals regarding their personal data, empowering them to exercise control over their information.

Volume 32, May 2024 ISSN 2581-5504

Data Protection Authority:

GDPR: Establishes independent supervisory authorities in each EU member state to enforce the regulation and oversee compliance.

DPDP: Expected to establish a Data Protection Authority (DPA) in India responsible for enforcing data protection laws, investigating violations, and imposing penalties.

Penalties:

GDPR: Imposes fines of up to €20 million or 4% of global annual turnover, whichever is higher, for serious violations.

DPDP: Likely to prescribe penalties for non-compliance, including fines and sanctions, based on the severity of the violation and the organization's turnover.

Cross-Border Data Transfers:

GDPR: Requires data transfers to countries outside the EEA to ensure an adequate level of protection or implement appropriate safeguards, such as standard contractual clauses or binding corporate rules.

DPDP: Expected to include provisions for cross-border data transfers, ensuring that personal data transferred outside India is adequately protected.

Extraterritorial Application:

GDPR: Applies to organizations outside the EU if they offer goods or services to individuals in the EU or monitor their behavior.

DPDP: May have provisions for extraterritorial application, potentially impacting foreign organizations processing personal data of Indian residents.

Challenges of GDPR and DPDPA

Compliance Complexity: One of the primary challenges for organizations is the complexity of compliance with GDPR and DPDPA requirements. Both regulations have extensive provisions and require organizations to implement various technical and organizational measures to ensure compliance. Understanding the nuances of these regulations and implementing necessary changes can be challenging, especially for smaller businesses with limited resources.

Data Governance: GDPR and DPDPA emphasize the importance of effective data governance practices, including data mapping, classification, and documentation. Organizations must have a clear understanding of the personal data they collect, process, and store, as well as the legal basis for processing and data subject rights associated with that data. Establishing robust data governance frameworks can be time-consuming and resource-intensive.

Volume 32, May 2024 ISSN 2581-5504

Consent Management: Obtaining valid consent for data processing is a key requirement under both GDPR and DPDPA. Organizations must ensure that consent mechanisms are transparent, specific, and freely given by data subjects. Managing consent preferences, providing opt-out mechanisms, and maintaining records of consent can be challenging, especially in complex data processing environments.

Data Security: GDPR and DPDPA mandate that organizations implement appropriate security measures to protect personal data from unauthorized access, disclosure, alteration, or destruction. Ensuring data security requires investments in cybersecurity infrastructure, encryption technologies, access controls, and regular security assessments. Organizations must also be prepared to respond effectively to data breaches and security incidents.

Rights are there in GDPR and DPDPA

Rights under GDPR:

- Right to access: Individuals have the right to obtain confirmation of whether their personal data is being processed and access to that data.
- Right to rectification: Individuals can request the correction of inaccurate or incomplete personal data.
- Right to erasure (right to be forgotten): Individuals can request the deletion of their personal data under certain circumstances.
- Right to restriction of processing: Individuals can request the limitation of the processing of their personal data under certain conditions.
- Right to data portability: Individuals can request to receive their personal data in a structured, commonly used, and machine-readable format and transmit it to another controller.
- Right to object: Individuals can object to the processing of their personal data based on specific reasons, such as processing for direct marketing purposes.

Rights related to automated decision-making and profiling: Individuals have the right not to be subject to decisions based solely on automated processing, including profiling, that produce legal effects concerning them or significantly affect them.

Rights under DPDP (expected to be similar to GDPR):

- Right to access
- Right to rectification
- Right to erasure
- Right to restriction of processing
- Right to data portability
- Right to object
- Rights related to automated decision-making and profiling

Volume 32, May 2024 ISSN 2581-5504

These rights empower individuals to have greater control over their personal data and ensure that their privacy is respected by organizations processing their information.

What Are the Compliance Challenges for GDPR and Indian PDPDA?

Both the GDPR (General Data Protection Regulation) and the Indian Personal Data Protection Act (PDPDA) present several compliance challenges for organizations. Here's an overview of some common challenges associated with each regulation:

Compliance Challenges for GDPR:

Complexity and Scope: The GDPR is a comprehensive regulation with complex requirements, making compliance challenging for organizations of all sizes, particularly those with limited resources or expertise in data protection.

Data Subject Rights: Ensuring compliance with data subject rights, such as the right to access, rectification, erasure, and data portability, requires organizations to establish robust processes and mechanisms for handling requests within the specified timelines.

Data Governance and Accountability: GDPR mandates that organizations implement appropriate technical and organizational measures to ensure data protection and demonstrate compliance. This includes conducting data protection impact assessments (DPIAs) and maintaining records of processing activities.

Cross-Border Data Transfers: Transferring personal data outside the European Economic Area (EEA) requires organizations to ensure an adequate level of protection or implement appropriate safeguards, such as standard contractual clauses or binding corporate rules.

Data Breach Notification: GDPR requires organizations to report data breaches to supervisory authorities within 72 hours of becoming aware of the breach. Ensuring timely and accurate breach notification can be challenging, especially for organizations with complex data environments.

Vendor Management: Organizations must ensure that their third-party vendors and service providers comply with GDPR requirements, which may involve conducting due diligence, negotiating data processing agreements, and monitoring vendor activities.

Regulatory Enforcement and Fines: GDPR empowers supervisory authorities to impose significant fines for non-compliance, which can amount to up to €20 million or 4% of the organization's global annual turnover, whichever is higher. Fear of regulatory enforcement and fines can be a significant compliance challenge for organizations.

Compliance Challenges for Indian PDPDA:

Data Localization: If the PDPDA includes provisions for data localization, organizations may face challenges in setting up infrastructure and systems to store and process personal data within India's borders.

Volume 32, May 2024 ISSN 2581-5504

Cross-Border Data Transfers: Similar to the GDPR, the PDPDA may impose restrictions on cross-border data transfers, requiring organizations to implement appropriate safeguards or obtain regulatory approvals for international data transfers.

Consent Management: Obtaining valid consent for data processing activities can be challenging, particularly in a diverse and culturally heterogeneous country like India. Organizations must ensure that consent is freely given, specific, informed, and unambiguous.

Regulatory Compliance Burden: Compliance with the PDPDA may impose additional administrative and compliance burdens on organizations, particularly small and medium-sized enterprises (SMEs) with limited resources and capabilities.

Enforcement Mechanisms: The effectiveness of the PDPDA will depend on the adequacy of its enforcement mechanisms and the capacity of regulatory authorities to investigate violations and impose penalties.

Harmonization with Other Laws: Ensuring harmonization and consistency between the PDPDA and other relevant laws and regulations, such as sector-specific data protection requirements, may pose challenges for organizations operating in regulated industries.

Public Awareness and Education: Building public awareness and understanding of data protection rights and responsibilities under the PDPDA will be essential for ensuring compliance and fostering a culture of data privacy in India.

In summary, both the GDPR and the Indian PDPDA present significant compliance challenges for organizations, ranging from technical and operational complexities to regulatory and legal requirements. Effective compliance requires a proactive approach, ongoing monitoring, and continuous improvement of data protection practices.

Future Scope

Global Impact: Both regulations are likely to influence data protection laws and practices globally. As countries around the world strive to enhance data privacy standards, they may look to GDPR and DPDPA as models for their own legislation.

Technological Advancements: With rapid advancements in technology, including artificial intelligence, big data analytics, and Internet of Things (IoT) devices, there will be evolving challenges and opportunities for data protection. Future revisions of GDPR and DPDPA may need to address these emerging technologies and their implications for privacy.

Cross-Border Data Transfers: As digital globalization continues, cross-border data transfers will remain a significant concern. Both GDPR and DPDPA include provisions for international data transfers, and future developments may involve more standardized approaches to facilitate data flows while ensuring adequate protection.

Enforcement and Compliance: The effective enforcement of GDPR and DPDPA is crucial for ensuring compliance and accountability. Regulatory authorities will continue to play a vital role

Volume 32, May 2024 ISSN 2581-5504

in monitoring and enforcing data protection laws, imposing fines and penalties for non-compliance, and promoting a culture of data privacy.

Data Governance and Accountability: Organizations will need to strengthen their data governance frameworks and accountability mechanisms to ensure compliance with GDPR, DPDPA, and other data protection regulations. This includes implementing privacy by design principles, conducting regular audits and assessments, and appointing data protection officers.

Limitation

Contextual Differences: The GDPR was designed for the European Union, while the Digital Personal Data Protection Act is specific to India. The legal, cultural, and socio-economic contexts in these regions differ, which may affect the interpretation and implementation of the laws.

Scope and Definitions: The definitions of key terms such as "personal data," "data subject rights," and "data processing" may vary between the GDPR and the Indian Act, leading to differences in their application and enforcement.

Enforcement Mechanisms: The GDPR has a well-established framework for enforcement, including regulatory authorities such as the European Data Protection Board and hefty fines for non-compliance. In contrast, the enforcement mechanisms in India may be less robust, impacting the effectiveness of the Act.

Compliance Burden: The compliance requirements under the GDPR are extensive and may pose a significant burden on organizations, especially small and medium-sized enterprises. The extent of the compliance burden under the Digital Personal Data Protection Act may differ, affecting its adoption and implementation.

Evolving Regulatory Landscape: Both the GDPR and the Indian Act are subject to amendments and interpretations over time. Changes in technology, legal precedents, and global data protection trends may influence the effectiveness and relevance of these laws.

International Data Transfers: The GDPR has specific provisions governing the transfer of personal data outside the EU, including requirements for adequate safeguards and data protection agreements. The Indian Act may have different provisions or lack clarity on international data transfers, posing challenges for cross-border data flows.

Conclusions

In conclusion, the Digital Personal Data Protection Act of India 2023 (DPDPA) and the General Data Protection Regulation (GDPR) represent significant milestones in the field of data protection and privacy regulation. While both aim to safeguard individuals' personal data and promote responsible data handling practices, there are notable differences between the two regulations.

Volume 32, May 2024 ISSN 2581-5504

The DPDPA, introduced by the Indian government, seeks to establish a comprehensive framework for the processing of digital personal data in India. It aims to balance individuals' rights to privacy with the legitimate interests of businesses and government entities in processing personal data. The DPDPA is designed to replace the existing patchwork of data protection laws and regulations in India and bring them in line with global standards.

On the other hand, the GDPR, implemented by the European Union, sets out stringent requirements for the collection, processing, and protection of personal data within the EU and the European Economic Area (EEA). It provides individuals with greater control over their personal data and imposes strict obligations on organizations handling such data, including enhanced transparency, accountability, and data subject rights.

Reference

1. EUDeligation (2017). EU-U.S. Privacy Shield. Retrieved from https://ec.europa.eu/info/law/lawtopic/data-protection/data-transfers-outside-eu/eu-us-privacy-shield_en
2. ersheds (2017). EU GDPR – Cross-Border Data Transfers. Retrieved https://www.evershedssutherland.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
4. "General Data Protection Regulation (GDPR)" - Official Website of the European Union Link: https://gdpr.eu/
5. "The Digital Personal Data Protection Act, 2023 (DPDPA)" - Government of India Official Gazette Link: [Insert link to the official document if available]
6. Cavoukian, Ann, and Daniel Castro. "Big data and innovation, setting the record straight: De-identification DOES work." (2015). Link: https://www.eff.org/files/2015/07/17/big_data_innovation.pdf
7. Chaudhary, Tanuj. "Explainer: India’s Personal Data Protection Bill, 2019." MediaNama. December 14, 2019. Link: https://www.medianama.com/2019/12/223-indias-personal-data-protection-bill-2019-explainer/
8. Singh, Ritambhara. "Data Protection Laws in India: A Critical Analysis." SSRN Electronic Journal. September 25, 2020. Link: https://ssrn.com/abstract=3691552
9. "A Comparative Analysis of the GDPR and India's Personal Data Protection Bill 2019." DataGuidance. December 16, 2020. Link: https://www.dataguidance.com/comparative-analysis-gdpr-indias-personal-data-protection-bill-2019
10. "India’s New Personal Data Protection Bill: Key Features, Analysis and Impact." DLA Piper. December 12, 2019. Link:
11. https://www.dlapiperdataprotection.com/index.html?t=law&c=IN&p=india_s_new_personal_data_protection_bill