Journal of Information Systems Engineering and Management
2025, 10(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Cross-Border Data Transfer Under Indian Data Protection Regimes With Special Reference To The Digital Personal Data Protection Act, 2023

Ms. Sonia Nath[1*], Dr. Rumi Dhar[2]

[1*]Research Scholar, Department of Law, Nagaland University (A Central University), Nagaland, India
sonia_rs2022@nagalanduniversity.ac.in.

[2]Assistant Professor, Department of Law, Nagaland University (A Central University), Nagaland, India
rumidhar@nagalanduniversity.ac.in.

Citation: Ms. Sonia Nath, et al. (2025) Cross-Border Data Transfer Under Indian Data Protection Regimes With Special Reference ToThe Digital Personal Data Protection Act, 2023, *Journal of Information Systems Engineering and Management*, *10*(3)

ARTICLE INFO

Received: 16 Nov 2024
Revised: 28 Dec 2024
Accepted: 08 Apr 2025

ABSTRACT

In an increasingly interconnected world, the seamless flow of cross-border data transfer has become integral to global business operations. It has raised significant legal and regulatory challenges in safeguarding individual privacy and data security. The paper delves into the evolving landscape of cross-border data transfer within the context of India's data protection regimes, with a special focus on the Digital Personal Data Protection Act 2023 (hereinafter referred to as DPDPA). The Act represents a significant legislative step towards enhancing the protection of personal data in cross-border transactions. The Act allows cross-border data transfer; however, the Central government can restrict such transfer. This study critically examines the provisions of the DPDPA and compares them with the provisions of international standard regulatory frameworks like the European Union General Data Protection Regulation. Through an analysis of key legal and regulatory developments and policies, the paper provides a comprehensive understanding of the current state of cross-border data transfer under Indian law.

Keywords: *Cross-Border Data Transfer, Data Privacy and Security, EU GDPR, and the Digital Personal Data Protection Act 2023.*

1. INTRODUCTION

The digital economy and the global nature of business operations have led to an exponential increase in cross-border data flows. Companies frequently practice cross-border data transfer for various purposes, including outsourcing, cloud computing, and global collaboration.[1] However, the legal considerations of cross-border data transfer have become increasingly important due to the potential risks and implications involved[2]. One of the main legal considerations of cross-border data transfer is the issue of data protection and privacy. Different countries have different laws, regulations, and mechanisms to safeguard personal data, and these laws can vary significantly in terms of scope, requirements, and enforcement mechanisms[3]. For example, the European

[1] Macmillan Kecj, Seharish Gillani, Ahmed Dermish, Jeremiah Grossman and Friederik Ruhmann of the UNCDF Policy Accelerator, "The role of cross-border data flows in the digital economy", July 2022, (https://web-assets.bcg.com/7a/2b/9a0cb4b545ad87cf7e901301ad27/en-uncdf-brief-cross-border-data-flows-2022.pdf) (accessed 5th July 2024).

[2] United Nations Conferences on Trade and Development (UNCTAD), "Data Protection Regulations and International Data Flows: Implications for Trade and Development", United Nations, New York and Geneva, April 2016, (https://unctad.org/system/files/official-document/dtlstict2016d1_en.pdf), (accessed 03rd July, 2024),

[3] Joshua P. Meltzer and Peter Lovelock, "Regulating for a Digital Economy Understanding the Importance of Cross-Border Data Flows in Asia", Global Economy & Development Working Paper 13, March 2018,

Journal of Information Systems Engineering and Management
2025, 10(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Union's General Data Protection Regulation (GDPR) sets strict rules for cross-border data transfer outside the EU, requiring specific safeguards and mechanisms to protect individual data rights.

The legal consideration of cross-border data transfer concerns intellectual property rights and trade secrets. Transferring data across borders can pose risks of intellectual property theft and unauthorized disclosure of valuable information[4]. As a result, many countries have established legal frameworks to protect intellectual property rights and trade secrets, and these laws may impose limitations on the cross-border transfer of certain types of data. So, it has become paramount for businesses and individuals engaging in cross-border data transfer to assess and comply carefully with the relevant laws and regulations[5]. This may involve implementing specific data protection measures, obtaining necessary permissions or certifications, and ensuring legal regulatory compliances of the countries involved in the data transfer.

The cross-border data transfer is complex and multifaceted, encompassing various issues related to data protection, national security, intellectual property rights, and trade secrets[6]. As the global digital economy[7] continues to grow, it is essential for businesses and individuals to be aware of and comply with the legal requirements governing cross-border data transfer to avoid potential legal risks and liabilities[8]. To mitigate the risk associated with cross-border data transfer, businesses operating in India must adopt robust data protection mechanisms and best practices. This may include conducting privacy impact assessments, implementing adequate security measures, and embracing data transfer agreements that provide adequate safeguards for transferred data[9]. Additionally, ensuring compliance with the evolving data protection laws and fostering a culture of data privacy and security awareness within organizations is crucial. The paper aims to explore the legal frameworks and challenges surrounding cross-border data transfer in India's data protection regime, focusing on safeguarding personal data while facilitating the free circulation of information across borders.

A. Research Objectives:

The primary objective of the paper is to critically examine the legal structure governing cross-border data transfer under Indian data protection regimes and
1. To understand the concept of cross-border data transfer and its significance within the frame of Indian data protection laws.
2. To analyze the legal and regulatory requirements for cross-border data transfer under the Digital Personal Data Protection Act 2023 and other relevant laws in India.
3. To identify the key challenges and concerns associated with cross-border data transfer under Indian data protection regimes.
4. To evaluate the effectiveness and adequacy of the current legal and regulatory framework in addressing the challenges and concerns related to cross-border data transfer.

B. Research Methodology

(https://www.brookings.edu/wp-content/uploads/2018/03/digital-economy_meltzer_lovelock_web.pdf), (accessed 5th July, 2024).

[4] *Supra* note 2.

[5] Asheef Iqubbal, "Impact of Barriers on Cross-Border Data Flow on Ease of Doing Digital Business in India', Discussion Paper, CUTS International, June 2022, (https://cuts-ccier.org/pdf/dp-impact-of-barriers-on-cross-border-data-flow-on-ease-of-doing-digital-business-in-india.pdf), (accessed 3rd July 2024).

[6] *Supra* note 2.

[7] Thomas Dewaranu, Glen Hodgson and Pingkan Audrine, "Policy Brief Regulating Cross Border Data Flows in the Development Context", T20 Indonesia, 2022, (https://www.t20indonesia.org/wp-content/uploads/2022/09/TF2_REGULATING-CROSS-BORDER-DATA-FLOWS-IN-THE-DEVELOPMENT-CONTEXT.pdf), (accessed 5th July 2024),

[8] Hunton & Williams, "Business Without Borders: The Importance of Cross-Border Data Transfer to Global Prosperity", U.S Chamber of Commerce, (https://www.huntonak.com/images/content/3/0/v3/3086/Business-without-Borders.pdf), (accessed 5th July, 2024).

[9] World Bank Group and CGAP, "Data Protection and Privacy for Alternative Data", GPFI-FCPL Sub-Group Discussion Paper-Draft, May 4, 2018, (https://www.gpfi.org/sites/gpfi/files/documents/Data_Protection_and_Privacy_for_Alternative_Data_WBG.pdf). (accessed 8th July 2024)

Journal of Information Systems Engineering and Management
2025, 10(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

A multi-disciplinary research methodology is adopted to address the research objectives outlined above. The research methodology for this paper involves:

1. Literature Review: A comprehensive review of relevant literature, including academic articles, books, reports, and legal sources, to gain a thorough understanding of the legal and regulatory framework for cross-border data transfer in India.

***2. Legal Analysis*:** An in-depth analysis of the Digital Personal Data Protection Act, 2023, Information Technology Act, 2000, IT Rule 2011, and other relevant legal frameworks pertaining to data protection and cross-border data transfer in India will be undertaken to identify the legal requirements and obligations for cross-border data transfer.

3. Comparative Analysis: A comparative analysis of the data protection laws and regulatory frameworks in other jurisdictions, particularly the European Union General Data Protection Regulation (GDPR), California Privacy Rights Act of 2020 (earlier California Consumer Privacy Act of 2018), Personal Information Protection Law of the People's Republic of China and the Personal Information Protection and Electronic Documents Act 2000 of Canada, to evaluate the adequacy and effectiveness of the Indian data protection regime in addressing cross-border data transfer concerns.

2. DATA PROTECTION LAWS IN INDIA

Today, data protection laws in India have evolved over time in response to the increasing importance and reliance on the internet. Both domestic and international developments have influenced the evolution of data protection laws in India and have been shaped by factors such as technological advancements and globalization. In the digital age, there is a need to balance the free flow of data and the protection of data in cross-border data transactions[10]. India's data protection laws primarily revolve around the Digital Personal Data Protection Act 2023[11]. The Act aims to regulate the process of handling personal data in India and shield individuals' right to privacy[12].

2.1. History and Development of Data Protection Laws in India

The first significant development in data protection laws in India came with the passage of the 'Information Technology Act of 2000'[13]. This legislation provided a legal framework for electronic transactions, digital signatures, and cybercrimes but did not specifically address personal data protection. It was not until 2011 that the government introduced the 'Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules'[14], which set out certain requirements for collecting, storing, and transferring sensitive personal data.

In 2017, the Supreme Court of India declared privacy as a fundamental right under part III of the Indian Constitution[15], which further strengthened the legal foundation for data protection in the country. This

[10] Rahul Matthan and Shreya Ramann, "India's Approach to Data Governance", (Data Governance, Asian Alternatives, How India and Korea Are Creating New Models and Policies),11-32 (Evan A Feigenbaum and Nelson ed., Carnegie Endowment for International Peace, August 2022,) (https://carnegieendowment.org/files/Data_Governance_v1.pdf), (accessed 2nd July, 2024)

[11] The Digital Personal Data Protection Act 2023 (No. 22 of 2023) Gazette of India, August 11, 2023, (https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf)

[12] Anirudh Burman, "Understanding India's New Data Protection Law", Carnegie India, October 03, 2023, (https://carnegieindia.org/2023/10/03/understanding-india-s-new-data-protection-law-pub-90624) (accessed 10th July 2024)

[13] The Information Technology Act 2000 (No. 21 of 2000) Gazette Notification, June 9th, 2000, (https://www.indiacode.nic.in/handle/123456789/1999).

[14] The Information Technology ((Reasonable Security practices and procedures and sensitive personal data or information) Rull, 2011, Gazette Notification, G.S.R. 313(E) April 11, 2011, (https://www.meity.gov.in/writereaddata/files/GSR313E_10511%281%29_0.pdf).

[15] Justice K.S Puttaswamy (Retd.) & Anr. Vs Union of India & Ors. (2017)10 SCC 1, AIR 2017 SC 4161.

Journal of Information Systems Engineering and Management
2025, 10(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

landmark decision paved the way for the drafting of a comprehensive data protection law, leading to the introduction of the Personal Data Protection Bill in 2019. The introduction of the ***Digital Personal Data Protection Act 2023*** brought about significant changes in the way cross-border data transfer is managed and regulated in India. The Digital Personal Data Protection Act 2023 establishes clear requirements for obtaining explicit consent from data subjects, ensuring adequate security measures for the protection of personal data, and imposing limitations on the sharing of sensitive personal data outside India[16].

In addition to domestic developments, the evolution of data protection laws in India has also been shaped by international influences. India is not a member of the European Union but has been influenced by the General Data Protection Regulation (GDPR), which sets out rules for data sharing outside the jurisdiction of the EU[17]. The GDPR has significantly impacted global data protection standards and has prompted countries like India to strengthen their own data protection laws to facilitate cross-border data transfers.

3. WHAT IS CROSS-BORDER DATA TRANSFER

In simple terms, cross-border data transfer means sharing personal sensitive data from one jurisdiction to another. Such transfer can be for advancing services across borders, fostering innovation, and enhancing public health, safety, and the collective welfare of society. On one side, the cross-border transfer of data boosts innovation and other services across the globe; and parallel, it raises the alarm for national security, safeguarding citizens' personal information to prevent misuse and fortifying domestic economic capacities in a progressively technological global landscape.

There is no specific legal definition of cross-border data transfer, but provisions relating to cross-border data transfer under different legal systems show the concern of various countries regarding the transfer of personal sensitive data over other jurisdictions. The 'European General Data Protection Regulation'[18] under Chapter 5 (Articles 44 to 50), the provisions related to the transfer of personal data to any other countries or international organizations are discussed. Article 44[19] of the EU GDPR provides general principles of transfer. Transferring personal data to a third country or international organization, whether it is in the process of being processed or intended for processing after being transferred, is only allowed when the controller and processor meet the requirements listed in EU GDPR chapter 5 and other relevant regulations.

Article 44 of EU DGPR- General Principles for Transfer:

> "*Any transfer of personal data which undergoing processing or are intended for processing after transfer to a third country or to an international organization shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this chapter are complied with by the controller and processor, including for onward transfer of personal data from the third country or an international organisation to another third country or to another international organization. All provisions of this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined*[20]."

The implementation of all the restrictions provided by the Regulation ensures that the level of protection guaranteed by this Regulation remains uncompromised. When the European Commission has concluded that the nation or organization in question provides sufficient data protection, only then can personal data be

[16] *Supra* note 12.
[17] Shakila Bu-Pasha, "Cross-Border Issues Under EU Data Protection Law with Regard to Personal Data Protection", Information & Communications Technology Law (Routledge Taylor & Francis Group) 2017, Vol 26, No. 3, pages 213-228, DOI: (https://doi.org/10.1080/13600834.2017.1330740, (https://www.tandfonline.com/doi/epdf/10.1080/13600834.2017.1330740?needAccess=true), (accessed 3rd July 2024)
[18] Regulation (EU) 2016/679 of the European Parliament and the Council of April 27, 2016, and repealing Directives 95/6/EC (General Data Protection Regulation), Official Journal of the European Union, (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679).
[19] *Ibid.*
[20] *Ibid.*

Journal of Information Systems Engineering and Management
2025, 10(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

transferred to a third country or international organization (Article 45[21] -***Transfer on the basis of an adequacy decision)***. This determination is made through an adequacy decision, which considers the laws and regulations in place in the recipient country or organization, as well as their enforcement mechanisms and the international commitments they have made regarding data protection.

In cases where a recipient country does not offer an adequate level of protection, then Article 46,[22] ***(Transfer subject to appropriate safeguard)*** provides mechanisms for ensuring that appropriate safeguards are in place for the transaction of personal data. On the other hand, Article 47 of EU GDPR (***Binding corporate rules)*** layout the legal framework for multinational companies to establish a set of binding rules for the transfer of personal data within their organization, and Article 50[23] ***(International cooperation for the protection of personal data)*** outlines the principle of international cooperation between the EU and other countries when it comes to the protection of personal data.

India has recognized the significance of protecting personal data and information privacy. The data protection regime in India is primarily governed by the 'Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011'[24], under the Information Technology Act, 2000[25]. Additionally, the Digital Personal Data Protection Act of 2023 proposes a comprehensive legal structure for the protection of individual data in India and regulates the process of cross-border data transfer. This framework introduces the obligations of data fiduciaries and data processors, particularly regarding the cross-border transfer of personal data[26]. Rule 7 ***(Transfer shows information***) of IT Rules 2011 and Section 16 ***(Provisions relating to processing of personal data outside India***) of the Digital Personal Data Protection Act 2023 show restrictions on cross-border data transfer.

3.1 Challenges and risks associated with Cross-Border data transfer

Cross-border data transfer has become essential to the global economy and society. However, this process is not without its risks and challenges, particularly in settings of a data protection legal framework. The challenges and risks accompanying cross-border data transfer are:

1) The risks associated with cross-border data transfer are the potential for data breaches[27] and unauthorized access to personal information. When data is transferred across borders, it becomes vulnerable to interception and exploitation by malicious actors.

2) When data is transferred across borders, it becomes subject to the laws and regulations of multiple jurisdictions, each with its own set of rules governing data protection. This fabricates a complex web of legal requirements that can be difficult to navigate and can end in the exposure of sensitive or confidential information to unauthorized parties.

---

[21] Article 45 of EU GDPR- Transfer on the basis of an adequacy decision: A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country or the international organization in question ensures an adequate level of protection. Such transfer shall not require any specific authorization, *Supra* note 18.
[22] *Supra* note 18.
[23] *Supra* note 18.
[24] The Information Technology ((Reasonable Security practices and procedures and sensitive personal data or information) Rull, 2011, Gazette Notification, G.S.R. 313(E) April 11, 2011, (https://www.meity.gov.in/writereaddata/files/GSR313E_10511%281%29_0.pdf).
[25] The Information Technology Act 2000 (No. 21 of 2000) Gazette Notification, June 9th, 2000, (https://www.indiacode.nic.in/handle/123456789/1999).
[26] Dr. Guru Prakash Paswan and Ruchi Singh, "*India's Digital Protection Bill: A Milestone in Data Protection and Global Competitiveness*", MyGov July 21, 2023, (https://blog.mygov.in/editorial/indias-digital-protection-bill-a-milestone-in-data-protection-and-global-competitiveness/), (accessed 10th July 2024).
[27] Data breach is a loss, unauthorised access to or disclosure of personal data as a result of a failure of the organization to effectively safeguard the data, OECD (April 6, 2011) Digital Economy Papers, No. 176, OECD Publishing, Paris, (DOI: https://doi.org/10.1787/5kgf09z90c31-en) (accessed 10 July 2024).

Journal of Information Systems Engineering and Management
2025, 10(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

3) One of the significant challenges associated with cross-border data transfer is the potential for legal and regulatory conflicts. Different countries have different standards and requirements for data protection, and these can sometimes conflict with one another.

4) Another challenge associated with cross-border data transfer is ensuring the competency of data protection standards in the recipient country. The recipient country's data protection laws standards are at par with or better than the standards prescribed. This requirement poses a significant challenge to the recipient country as privacy laws vary widely across different jurisdictions.

5) Cross-border data transfer can also raise concerns about the misuse of data for surveillance. Particularly when data is transferred to countries with less stringent privacy protections.
The cross-border transfer of data presents numerous risks and challenges that must be carefully considered and addressed from a legal and regulatory perspective. By developing common standards and mechanisms for data protection across borders and by taking proactive measures to mitigate risks, the benefits of cross-border data transfer can be realized while minimizing the potential harm.

3.2. Legal requirement for Cross-Border data transfer

The legal requirement for cross-border data transfer is for both countries to adhere to the principles of cross-border data transfer. The General Data Protection Regulation (GDPR) is the primary legislation that governs the transfer of personal data outside the EU and the European Economic Area (EEA)[28]. The GDPR sets out strict mechanisms for the transfer of personal data and ensures the protection of individuals' fundamental rights to privacy. The GDPR provides alternative mechanisms for legitimizing cross-border data transfers. These include standard contractual clauses between the data sharer, binding corporate rules within a multinational enterprise, or certification mechanisms approved by supervisory authorities. These mechanisms are designed to ensure that the personal data transferred outside the EU is subject to equivalent safeguards as those provided within the EU[29].

According to the provisions laid down in the Digital Personal Data Protection Act 2023, there is no specific mechanism for cross-border data transfer; however, the central government has the power to restrict the transfer of cross-border data to certain countries. So, by implementing GDPRs like legal provisions for such data transfer under India's legal framework, the mechanism can be strengthened.

4. INDIAN LEGAL FRAMEWORK FOR CROSS-BORDER DATA TRANSFER

India has seen tremendous growth in the digital economy, with more and more businesses relying on cross-border data transfer for their operations. The Indian legal framework for cross-border data transfer plays a crucial role in governing the mechanism for cross-border data transfer and ensuring the protection of sensitive information[30]. The legal considerations surrounding cross-border data transfer under India's data protection regime encompass various aspects, including the permissible grounds for cross-border data transfer and the role and obligations of data fiduciaries and data processors for obtaining explicit consent from data subjects[31]. Furthermore, the adequacy of data protection measures in the recipient country and the probable effect on the rights of data subjects are paramount legal considerations that must be addressed.

Under the Indian legal framework, we have the Information Technology Act 2000, Information Technology (Reasonable security and procedures under sensitive personal data or information) Rules, 2011, RBI circular

[28] Sebastian Allerelli, "What is a GDPR cross border data transfer?", Safe Online August 22, 2023, (https://bysafeonline.com/what-is-a-gdpr-cross-border-data-transfer/) (accessed 7th July 2024)
[29] *Ibid.*
[30] CII-TATA Communication Centre for Digital Transformation, "Navigating Data Privacy in Digital India Digital Personal Data Protection Act, 2023: Industry Impact and Roadmap to Compliance", Protiviti Global Business Consulting, 2023, (https://www.protiviti.com/sites/default/files/2023-08/digital_personal_data_protection_act_2023.pdf) (accessed 2nd July 2024),
[31] Soham Choudhury, Koushi Sinha and Saikat Mondal, "Cross-Border Data Transfers: Legal Frameworks and Implications", Lexplosion, Aug 1, 2023, (https://lexplosion.in/cross-border-data-transfers-legal-frameworks-implications/) (accessed 3rd July 2024).

Journal of Information Systems Engineering and Management
2025, 10(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

in the context of financial transactions and the Digital Personal Data Protection Act 2023. The existing laws and regulations provide a foundation for governing data transfer, and further clarity and consistency are needed to ensure effective regulation and cross-border data transfer. The existing Indian legal framework for cross-border data transfer is as follows:

4.1. The Digital Personal Data Protection Act 2023[32]

The Digital Personal Data Protection Act 2023 is an important piece of legislation that aims to safeguard the personal data of individuals in the digital age. With the intense use of technology and the internet, the need for such legislative protection has become even more crucial. The Act contains various provisions to shield sensitive personal data from illegitimate access, use, handling, and transfer. The Digital Personal Data Protection Act 2023 aims to provide a comprehensive framework for the protection of personal data while facilitating cross-border data transfer. Cross-border data transfer plays a crucial role in the global flow of information, enabling businesses to operate internationally and facilitating innovation and collaboration across borders. However, it also raises concerns regarding the protection of personal data, particularly in the context of data privacy and security. The Digital Personal Data Protection Act 2023 strikes a balance between facilitating cross-border data transfer and ensuring the privacy and security of personal data.

One of the key provisions of the Act is the requirement for organizations to obtain ***"explicit consent"***[33] from individuals before transferring their personal data across borders. This is an important safeguard, as it ensures that individuals have control over how their data is used and shared, and it helps to prevent the unauthorized or unlawful transfer of data to jurisdictions with weaker data protection laws. The Act sets out guidelines for protection of data transfer, ensuring that personal data is adequately protected when transferred outside the jurisdiction. It requires organizations to assess the level of protection in the recipient country and implement appropriate safeguards to ensure the security and privacy of the transferred data.

Section 16[34] of the Digital Personal Data Protection Act 2023 deals with the provisions relating to cross-border data transfer. According to this section, extraterritorial data transfer is allowed except for those countries where the central government can restrict it through notifications. However, there are no strict guidelines or criteria that need to be followed for extra-jurisdictional data transfer. So, India needs to set up some tests for cross-border data transfer, which other countries have in their laws and regulations, such as adequate data protection security, compliance with the Indian data protection laws, standard business contracts between the countries, and data localization in India.

On the other hand, the GDPR, implemented by the European Union, is one of the most comprehensive and stringent data protection regulations worldwide. The GDPR places restrictions on cross-border data transfer, allowing transfers only to countries or international organizations that provide an adequate level of data protection. Organizations are required to adhere to specific legal mechanisms when transferring personal data to countries outside the EU, such as using standard contractual clauses or binding corporate rules. The GDPR also emphasizes the rights of data subjects and the accountability of organizations in ensuring the lawful and secure transfer of personal data. If we compare ***Section 3***[35] ***(Application of Act)*** of the Digital Personal

[32] The Digital Personal Data Protection Act 2023 (No. 22 of 2023) Gazette of India, August 11, 2023, (https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf)
[33] The Digital Personal Data Protection Act 2023, s 6(1) The consent given by the Data Principal shall be free, specific, informed, unconditional and unambiguous with a clear affirmation action, and shall signify an agreement to the processing of her personal data for the specified purpose and be limited to such personal data as is necessary for such specified purpose. *Supra* note 32.
[34] The Digital Personal Data Protection Act 2023, s 16 (1) of the Digital Personal Data Protection Act 2023 (Special Provisions): The Central Government may, by notification, restrict the transfer of personal data by a Data Fiduciary for processing to such country or territory outside India as may be so notified.
(2) Nothing contained in this section shall restrict the applicability of any law for the time being in force in India that provides for a higher degree of protection or restriction on the transfer of personal data by a Data Fiduciary outside India in relation to any personal data or Data Fiduciary or class thereof. *Supra* note 32.
[35] The Digital Personal Data Protection Act 2023, s 3 - Subject to the provisions of this Act, it shall- (a) apply to the processing of digital personal data within the territory of India where the personal data is collected-

Journal of Information Systems Engineering and Management
2025, 10(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Data Protection Act 2023 and ***Article 3***[36] ***(Territorial scope)*** of the European Union General Data Protection Regulation, the provisions relating to the applicability of the data protection laws show that India's data protection laws lack extraterritorial applicability.

The General Data Protection Regulation applies to any business that processes the personal data of EU residents, regardless of where the business is located. This means that even non-EU businesses are subject to GDPR if they handle EU residents' personal data. In contrast, the Digital Personal Data Protection Act 2023 only applies to businesses operating within the domain of the country where the legislation is enacted. This limitation can create loopholes for multinational corporations to exploit, leaving individuals' personal sensitive data vulnerable to exploitation and misuse. Secondly, if we compare the provisions relating to data breach notification between the Digital Personal Data Protection Act 2023 and the EU General Data Protection Regulation, Article 33[37] GDPR ***"Notification of a personal data breach to the Supervisory Authority"*** mandates that businesses notify relevant authorities and affected persons of a data breach within 72 hours of becoming aware of the breach. This prompt notification is crucial for an individual to grasp the precautions to protect their personal data and mitigate potential harm. However, Section 8 (6)[38] of the Digital Personal Data Protection Act 2023 does not have clear and strict requirements for data breach notification, leaving individuals in the dark about potential risks to their personal data.

4.2. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rule 2011[39]

This Rule is commonly known as IT Rule 2011, and the provisions relating to cross-border data transfer are an important aspect of the legislation, as they pertain to the transfer of extra-territorial personal data. These Rules are structured to ensure that the data rights of individuals remain protected even if their personal information is transferred to any other country.

The IT Rule 2011 permits cross-border data transfer only if the destination country has a significant level of data protection mechanism. This means that the recipient country must be deemed to be at par with the standard set out in the IT Rule. If the recipient country does not have a satisfactory level of data protection framework, then the transfer of such information is only permitted if the individual has explicit consent to such

(i) in digital form; or
(ii) in non-digital form and distinguished subsequently;
(b) also apply to processing of digital personal data outside the territory of India if such processing is in connection with any activity related to offering of goods or services to Data Principal within the territory of India.

[36] Article 3 GDPR- Territorial scope- 1. This regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.
2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subject in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.
3. The Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law. *Supra* note 18.

[37] Article 33 GDPR- Notification of a personal data breach to the supervisory authority- (1)In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedom of natural person. Where the notification to the supervisory authority is not made within 7 hours, it shall be accompanied by reason for the delay. *Supra* note 18.

[38] The Digital Personal Data Protection Act 2023, s 8(6)-In the event of a personal data breach, the Data Fiduciary shall give the Board and each affected Data Principal, intimation of such breach in such form and manners as may be prescribed. *Supra* note 32.

[39] The Information Technology ((Reasonable Security practices and procedures and sensitive personal data or information) Rull, 2011, Gazette Notification, G.S.R. 313(E) April 11, 2011, (https://www.meity.gov.in/writereaddata/files/GSR313E_10511%281%29_0.pdf).

Journal of Information Systems Engineering and Management
2025, 10(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

transfer (Rule 7[40]), and the Rule 6[41] IT Rule 2011 also requires organizations to disclose that personal data will be transferred internationally. This must be disclosed to the person before their data is transferred, and they must be informed of the potential risk involved in transferring their data to a country with fewer data protection laws.

Overall, the provisions relating to cross-border data transfer under the IT Rule 2011 are designed to protect the data protection rights of individuals when data is transferred across the border. By outlining the conditions under which cross-border data transfer is permissible and security measures that must be taken, the IT Rule 2011 ensures that an individual's data is handled responsibly and according to procedures laid down in the legal structure. These safeguard an individual's personal information regardless of where it is being transferred.

4.3. The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016[42]

This is a significant piece of legislation that governs the use and protection of Aadhaar data. In the age of globalization and digital connectivity, it is crucial to address the issues of cross-border data transfer and its implications for privacy and security. The Aadhaar Act does not specifically mention provisions that deal with cross-border data transfer. However, the Act contains certain principles and safeguards for protecting Aadhaar data, which implicitly affect cross-border data transfer. One important aspect of the Act is the provision for obtaining consent from individuals for the processing of their Aadhaar data. The Act also mandates UIDAI to take necessary precautionary measures to maintain the security and confidentiality of Aadhaar data, which includes preventing unauthorized access and disclosure of such data. These provisions are essential in the context of cross-border data transfer, as they underline the need for robust data protection measures during the transfer process.

Furthermore, the Aadhaar Act imposes strict penalties for unauthorized access, use, and disclosure of Aadhaar data. Provisions relating to protecting personal information are discussed under Section 28,[43] which ensures

[40] Rule 7 of IT Rule 2011- Transfer of information- A body corporate or any person on its behalf may transfer sensitive personal data or information including any information, to any other body corporate or a person in India, or located in any other country, that ensure the same level of data protection that is adhered to by the body corporate as provided for under these Rules. The transfer may be allowed only if it is necessary for the performance of the lawful contract between the body corporate or any person on its behalf or where such person has consented to data transfer. *Supra* note 39.

[41] Rule 6 of IT Rule 2011- Disclosure of information-(1) Disclosure of sensitive personal data or information by a body corporate to any third party shall require prior permission from the provider of such information, who has provided such information under lawful contract or otherwise, unless such disclosure has been agreed to the contract between the body corporate and provider of information, or where the disclosure is necessary for compliance of a legal obligation. *Supra* note 39.

[42] The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services Act, 2016, (No. 18 of 2016), Gazette Notification March 25th, 2016, (https://uidai.gov.in/images/Aadhaar_Act_2016_as_amended.pdf).

[43] The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services Act, 2016, s 28 Security and Confidentiality of information- (1) The Authority shall ensure the security of identify information and authentication records of individuals. (2) Subject to the provisions of this Act, the Authority shall ensure confidentiality of identity information and authentication records of individuals. (3) The Authority shall take all necessary measures to ensure to ensure that information in the possession or control of the Authority, including information stored in the Central Identities Data Repository, is secured and protected against access, use or disclosure not permitted under this Act or regulations made thereunder, and against accidental or intentional destruction, loss or damage.
(4) Without prejudice to sub-section (1) and (2), the Authority shall- (a) adopt and implement appropriate technical and organisational security measures;
(b) ensure that the agencies, consultant, advisors or other persons appointed or engaged for performing any function of the Authority under this Act, have in place appropriate technical and organizational security measures for the information; and
(c) ensure that the agreements or arrangements entered into with such agencies, consultants, advisors or other persons, impose obligations equivalent to those imposed on the Authority under this Act, and require such agencies, consultants, advisors and other persons to act only on instructions from the Authority.

Journal of Information Systems Engineering and Management
2025, 10(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

that sensitive personal information stored in the Aadhaar database is not misused or shared. It establishes the necessary safeguards to protect the privacy and security of Aadhar data. The Act emphasized the need to obtain consent, ensure data security, and impose penalties for unauthorized disclosure of Aadhar data.

Section 29 [44] of the Aadhaar Act, imposes limitations on the transfer of data from the Aadhaar ecosystem, but the Act does not have any direct provisions dealing with cross-border data transfer. The Act reflects that they directly impact the transfer of Aadhaar data across the border. In addition to the Aadhaar Act, the recent judgement of the Supreme Court of India in the case of ***Justice K S Puttaswamy (Retd) v Union of India***[45] has further strengthened the privacy rights of individuals in India. The judgement recognized the right to privacy as a fundamental right and laid down principles for protecting personal data. These principles significantly impact cross-border data transfer, as they emphasize the need for stringent data protection measures and the prerequisite condition for valid and informed consent from individuals for the transfer of their personal information.

4.4. The Information Technology (Amendment) Act, 2008[46]

The Information Technology (Amendment) Act of 2008 is a crucial piece of legislation in India that governs aspects of electronic commerce, information security, and cybercrime. The IT Amendment Act does not have any specific section that deals with cross-border data transfer. However, the Act contains certain provisions for protecting information, which implicitly affects cross-border data transfer. Section 69[47] of the Act, ***"Power to issue directions for interception or monitoring or decryption of any information through any computer resource"*** empowers the Indian government to intercept, monitor, and decrypt any information transmitted through any computer resources if deemed necessary for national security or public order. However, this provision has often been criticized for its potential to infringe upon the privacy rights of individuals. The provision of the Information Technology Amendment Act 2008 brought about significant changes in the landscape of information technology in India.

(5) Notwithstanding anything contained in any other law for the time being in force, and save as otherwise provided in this Act, the Authority or any of its officers or other employees or any agency that maintains the Central Identification Data Repository shall not, whether during his service or thereafter, reveal any information stored in Central Identities Data Repository or authentication record to anyone;
Provided that an Aadhar number holder may request the Authority to provide access to his identity information excluding his core biometrics information in such manner as may be specified by regulations. *Supra* note 42.

[44] Section 29- Restriction on sharing information- (1) No core biometric information, collected or created under this Act, shall be- (a) shared with anyone for any reason whatsoever; or
(b) used for any purpose other than generation of Aadhar numbers and authentication under this Act.
(2) The identity information, other than one biometric information, collected or created under this Act may be shared only in accordance with the provisions of this Act and in such manner as may be specified by regulations. *Supra* note 42.

[45] Justice K S Puttaswamy (Retd) v Union of India (2019) 1 SCC 1

[46] The Information Technology (Amendment) Act, 2008 (No. 10 of 2009), Gazette Notification Feb 5th, 2009, (https://www.indiacode.nic.in/bitstream/123456789/15386/1/it_amendment_act2008.pdf)

[47] The Information Technology (Amendment) Act, 2008, s 69- Power to issue directions for interception or monitoring or decryption of any information through any computer resource- (1) Where the Central Government or a State Government or any of its officers specially authorized by the Central Government or a State Government, as the case may be, in this behalf may, if satisfied that it is necessary or expedient so to do, in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign State or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigating of any offences, it may subject to the provisions of the sub-section(2), for reason to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource. *Supra* note 46.

Journal of Information Systems Engineering and Management
2025, 10(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

One of the notable provisions of the Act is Section 72,[48] ***"Penalty for Breach of Confidentiality and Privacy***" and Section 72A,[49] ***"Punishment for disclosure of information in breach of lawful contract".*** Section 72[50] safeguards personal information and data. The act addressed the need to safeguard the personal data of individuals and ensure that it is not misused or compromised during cross-border transfer. It imposes a legal duty on organizations and individuals to afford protection to sensitive personal data and restrict unauthorized disclosure of information.

5. GLOBAL LAWS ON CROSS-BORDER DATA TRANSFER

Cross-border data transfer is a complex and evolving area of law that requires careful consideration of privacy, security, and international cooperation. Some countries have established laws and regulations to govern cross-border data transfer, while some are in the process. Despite the efforts made by various countries to regulate cross-border data transfer, there is a gap in harmonization and consistency across different jurisdictions. The lack of uniformity creates compliance challenges for multinational organizations' free data flow. For example, the Asia Pacific Economic Cooperation (APEC) privacy framework is a regional initiative that promotes interoperability and mutual recognition of data protection laws among APEC members. This framework encourages member economies to adopt principles and mechanisms for facilitating cross-border data transfer while protecting personal information[51]. Let's discuss some of the important global legislation/regulations on cross-border data transfer and how Indian laws distinguish from other countries:

5.1. European Union General Data Protection Regulation (GDPR) 2018[52]

The European Union General Data Protection Regulation is one of the most influential and far-reaching pieces of legislation in the world of data protection and privacy. It has a profound impact on cross-border data transfer, which is an essential part of today's global economy. One of the primary drawbacks of the Digital Personal Data Protection Act 2023 is its lack of extraterritorial applicability. Regardless of the location of the business, the GDPR is applicable to any entity that handles the personal data of EU citizens[53]. This means that even non-EU businesses are subject to the GDPR if they handle the personal data of EU residents.

One of the key provisions of the GDPR is the idea of adequate protection for personal data. Article 45[54] the GDPR provides that personal data may only be transferred to a third country (outside the EU) if the recipient country ensures sufficient protection and security. This means that the third country's data protection regulations and practices must be at par with those of the EU to confirm the privacy and security of the data

[48] The Information Technology (Amendment) Act, 2008, s 72-Penalty for Breach of Confidentiality and Privacy- Save as otherwise provided in this Act or any other law for the time being in force, if any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years or with fine which may extend one lakh rupees, or with both. *Supra* note 46.

[49] The Information Technology (Amendment) Act, 2008, s 72A- Punishment for Disclosure of Information in Breach of Lawful Contract (Inserted vide ITAA-2008). Save as otherwise provided in this Act or any other law for the time being in force, any person, including an intermediary who, while providing services under the terms of a lawful contract, has secured access to any materials containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person shall be punished with imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both. *Supra* note 46.

[50] *Supra* note 49.

[51] APEC Internet and Digital Economy Roadmap (AIDER), Agenda Item, 22017/CSOM/006, available at: https://www.apec.org/groups/committee-on-trade-and-investment/digital-economy-steering-group

[52] Regulation (EU) 2016/679 of the European Parliament and the Council of April 27, 2016, and repealing Directives 95/6/EC (General Data Protection Regulation), Official Journal of the European Union, (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679).

[53] Deloitte, "Guide to the cross-border transfer of personal data in the GDPR", (https://www2.deloitte.com/al/en/pages/legal/articles/gdpr.html) (accessed 15th July 2024).

[54] *Supra* note 53.

Journal of Information Systems Engineering and Management
2025, 10(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

being transferred. Article 46[55] of the GDPR outlines several mechanisms that organizations can use to guarantee personal data protection when transferring it to a third country or international organization. These mechanisms include ***binding corporate rules***[56], standard data protection clauses adopted by the Commission, contractual clauses approved by the Competent Authority (competent supervisory authority), codes of conduct, and ***certification mechanisms***[57]. By using these appropriate safeguards, organizations can corroborate that the personal data they transfer across borders is adequately protected, even when it is outside the EU and European Economic Area. In cases where no adequacy decision[58] has been made by the European Commission regarding data protection standards in the third country; Article 46 requires that the data controller or processor provide suitable guarantees to confirm the protection of personal data[59].

The provisions of Article 46 serve as a powerful tool for promoting international cooperation and harmonization of cross-border data transfer. By carrying out standards mechanisms requiring adequate protection of personal data, the GDPR encourages global adherence to high data protection standards. This will benefit not only individuals within the EU but also create a more consistent and predictable regulatory environment for businesses and organizations operating internationally. Article 47[60] of the GDPR encourages

[55] Article 46 GDPR- Transfers subject to appropriate safeguards-(1) In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organization only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. *Supra* note 52.

[56] PWC, "Binding Corporate Rules the General Data Protection Regulation", (https://www.pwc.com/m1/en/publications/documents/pwc-binding-corporate-rules-gdpr.pdf) (accessed 15th July 2024).

[57] European Commission, "What rules apply if my organization transfer data outside the EU?", An Official website of the European Union, (https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_en) (accessed 9th July, 2024).

[58] European Commission, "Question & Answer: EU-US Date Privacy Framework", (https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3752) (accessed 10th July 2024).

[59] Data Protection Commission, "Transfer of Personal Data to Third Countries or International Organisations", (https://www.dataprotection.ie/en/organisations/international-transfers/transfers-personal-data-third-countries-or-international-organisations), (accessed 23rd July, 2024).

[60] Article 47 GDPR-Binding Corporate Rules- 1. The competent supervisory authority shall approve binding corporate rules in accordance with the consistency mechanism set out in Article 63, provided that they:
(a) are legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees; (b) expressly confer enforceable rights on data subjects with regard to the processing of their personal data; (c) fulfil the requirements laid down in paragraph 2.
2. The binding corporate rules referred to in paragraph 1 shall specify at least:
(a) the structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members; (b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purpose, the type of data subjects affected and the identification of the third country or countries in question; (c) their legally binding nature, both internally and externally;
(d) the application of the general data protection principles, in particular purpose limitation, data minimization, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules;
(e) the rights of data subjects in regard to processing and the means to exercise those rights, including the right not to be subject to decisions based solely on automated processing, including profiling in accordance with Article 22, the right to lodge a complaint with the competent supervisory authority and before the competent courts of the Member States in accordance with article 79, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;
(f) the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member concerned not established in the Union; the controller or the processor shall be exempt from the liability, in whole or in part only if proves that the member is not responsible for the event giving rise to the damage;
(g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e,) and (f) of this paragraph is provided to the data subjects in addition to Article 13 and 14;

Journal of Information Systems Engineering and Management
2025, 10(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

a consistent approach to data protection within multinational organizations. This is beneficial not only for the individuals whose data is being processed but also for the organizations themselves, as it helps to build trust and confidence in their data handling practices. Furthermore, the GDPR also allows cross-border data transfer in specific situations where derogations apply. The GDPR specifies certain circumstances where the transfer may take place without the need for specific authorization. These derogations include situations where the data subject has explicitly consented, where such transfer is necessary for the execution of a contract between the data subject and the controller, or where the transfer is obligatory for the public interest (Article 49[61]).

Article 47 of the EU General Data Protection Regulation (GDPR) relates to the binding corporate rules for data protection. Article 47 of the GDPR sets out the requirements for BCRs (Binding Corporate Rules) to be considered valid. These requirements include the need for the rules to be legally binding and enforceable, to cover all aspects of the GDPR, and to provide adequate rights for data subjects. The "***binding corporate rules"*** (BCRs) are a set of internal rules governing data protection within a multinational corporation. These rules must be legally binding and apply to all the entities within the corporate group, including subsidiaries and affiliates. BCRs are a way for organizations to ensure consistent data protection across their operations, regardless of where the data is being processed. Additionally, the BCRs must be approved by the relevant data

(h) the tasks of any data protection officer designated in accordance with Article 37 or any other person or entity in charge of the monitoring compliance with the binding corporate rules within the group of undertakings, or group of enterprises engaged in a joint economic activity, as well as monitoring training and complaint handling;
(i) the complaint procedures;
(j) the mechanism within the group of undertakings, or group of enterprise engaged in a joint economic activity for ensuring the verification of compliance with the binding corporate rules. Such mechanisms shall include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. Results of such verification should be communicated to the person or entity referred to in point (h) and the board of the controlling undertaking of a group of undertaking, or of the group of enterprises engaged in a joint economic activity, and should be available upon request to the competent supervisory authority;
(k) the mechanisms for reporting and recording changes to the rules and reporting those changes to the supervisory authority;
(l) the cooperation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, or group of enterprises engaged in a joint economic activity, in particular by making available to the supervisory authority the results of verifications of the measures referred to in point (j)
(m) the mechanism for reporting to the competent supervisory authority any legal requirement to which a member of the group of undertakings, or group of enterprises engaged in a joint economic activity is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules; and (n) the appropriate data protection training to personnel having permanent or regular access to personal data. *Supra* note 52.

[61] Article 49 GDP- Derogation for specified situations- 1. In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguard pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organization shall take place only on one of the following conditions:(a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risk of such transfer for the data subject due to the absence of an adequacy decision and appropriate safeguards;
(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
(d) the transfer is necessary for important reasons of public interest;
(e) the transfer is necessary for the establishment, exercise or defence of legal claims;
(f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;
(g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case. *Supra* note 52.

protection authority in the EU[62]. By setting out the requirements for binding corporate rules, this provision helps to create a more harmonized approach to data protection within multinational organizations, ultimately benefiting both data subjects and businesses.

The General Data Protection Regulation (GDPR) in the European Union and Indian data protection laws present major differences in their approaches to cross-border data transfer. These variations encompass the legal requirements, regulatory authorities, penalties for non-compliance, distinct legal frameworks and regulatory approaches adopted by both regions. The Indian law reflects the government's effort to assert greater control over the processing and storage of personal data, while the GDPR emphasizes the application of global data protection standards and includes more severe penalties for non-compliance.

5.2. California Privacy Rights Act of 2020[63] (earlier California Consumer Privacy Act of 2018):[64]

California data protection laws, specifically the California Consumer Privacy Act (CCPA), 2018, last amended in 2020 by the California Privacy Rights Act 2020 (CPRA), do not contain direct provisions relating to cross-border data transfer[65]. The Act does not restrict cross-border data transfer, whereas if we consider EU GDPR, such transfer is valid if it follows transfer mechanisms such as Binding Corporate Rules, Contract Clauses, etc.[66] Under the California Privacy Rights Act 2020, cross-border data transfer to a third party outside of California is subject to certain requirements.

The CCPA defines "***sale***"[67] broadly to include the transfer of personal information for valuable consideration. If a business sells personal information to third parties for valuable consideration, it must provide consumers with the opportunity to "***opt-out***"[68] of the sale of their personal information. The CCPA does not list the legal grounds based on which businesses can collect and sell personal information. It only provides that businesses must obtain the consent of consumers when they enter into a scheme that gives financial incentives on the basis of the personal information provided[69]. Additionally, the California Privacy Rights Act 2020[70] requires businesses to disclose in their privacy policies whether they sell personal information and provide a clear and

[62] Article 45 of EU GDPR- Transfer on the basis of an adequacy decision: A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country or the international organization in question ensures an adequate level of protection. Such transfer shall not require any specific authorization. *Supra* note 52.

[63] California Privacy Rights Act, Cal. Civ. Code §§ 1798.100 et seq (West 2020), (https://oag.ca.gov/system/files/initiatives/pdfs/19-0017%20%28Consumer%20Privacy%20%29.pdf).

[64] California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 et seq (West 2018), (https://cppa.ca.gov/regulations/pdf/cppa_act.pdfs).

[65] Cooley, "Cross-Border Data Transfer: PIPL vs. GDPR vs. CCPA", April 11, 2022, (accessed Dec 12, 11:00 P.M), (https://cdp.cooley.com/cross-border-data-transfers-pipl-vs-gdpr-vs-ccpa/).

[66] Data Guidance, "Comparing privacy laws: GDPR v CCPA, (accessed Dec 10, 2023, 10:00 P.M), (https://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf).

[67] California Privacy Rights Act 2020, s 1, 1798.140 (ad) (1) "sell", "selling", "sale", or "sold" means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communication orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for monetary or other valuable consideration, or otherwise for a commercial purpose, including but not limited to cross-context behavioural advertising. *Supra* note 63.

[68] California Privacy Rights Act 2020, s 9. 1798.120 - Right to Opt-Out of sale of Personal Information and sensitive Data Profiling. (a) A consumer shall have the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information. This right may be referred as the right to opt-out. *Supra* note 63.

[69] Data Guidance, "Comparing privacy laws: GDPR v CCPA", (https://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf) (accessed 10th July 2024).

[70] *Supra* note 63.

Journal of Information Systems Engineering and Management
2025, 10(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

conspicuous link on their homepage titled "***Do Not Sell My Personal Information***"[71] which allows consumers to opt out of the sale of their personal information. So, these conditions indirectly affect the transfer of cross-border data.

5.3. Personal Information Protection Law of the People's Republic of China 2021[72]

The Personal Information Protection Law (PIPL) is a comprehensive data protection legislation recently passed by the People's Republic of China. China's Personal Information Protection Law (PIPL) has introduced several provisions pertaining to cross-border data transfers, which have significant implications for how personal data is handled and protected[73]. The China PIPL introduces a requirement for data exporters to conduct a security assessment before transferring personal information to overseas entities. This assessment is intended to evaluate the data recipient's data protection capabilities and make sure that the transfer meets the legal obligations under the PIPL[74]. Additionally, the law requires data exporters to enter into a written contract with the data recipient, specifying the purpose, type, and scope of the personal information transfer. These provisions are aimed at safeguarding personal information during cross-border transfers and ensuring that data exporters remain accountable for the data they transfer.

Under the China Personal Information Protection Law, the State Cyberspace Administration is empowered to formulate and issue measures for regulating cross-border data transfers. This includes establishing a list of countries and regions that meet the requirements for cross-border data transfers, as well as issuing licenses for data transfers to entities in countries or regions that are not on the list. These measures provide a clear framework for regulating cross-border data transfers and ensuring that personal information is adequately protected when transferred outside of China[75].

Chapter 3 of China Personal Information Protection Law (Rules on Provision of Personal Information Across Border) deals with provisions relating to cross-border data transfer, along with obtaining consent, companies must also comply with certain requirements when transferring personal data outside of China. These requirements include conducting a security assessment to ensure that the recipient of the data has the necessary security measures for the data. This assessment is intended to prevent data breaches and unauthorized access to personal information. Furthermore, companies are required to enter into agreements with the recipients that specify the justification for which the data is being transferred and the accountability

[71] California Privacy Rights Act 2020, s 12. 1798.120 – Sale of Personal Information and Use of Personal Information for Advertising and Marketing Requirements. (a) (1) Provide a clear and conspicuous link on the business's internet homepage(s), titled "Do Not Sell My Personal Information," to an internet webpage that enables a consumer, or a person authorized by the consumer, to opt-out of the sale of the consumer's personal information, and in addition, an easily accessible link that allows consumers to opt-out of the use or disclosure of the consumer's sensitive personal information for advertising and marketing provided that a business may also utilize a single, clearly-labelled link on the business's homepage(s), if such link allows a consumer easily to opt-out of the sale of the consumer's personal information and to opt out of the use or disclosure of the consumer's sensitive persona information for advertising and marketing. A business shall not require a consumer to create an account in order to direct the business not to sell the consumer personal information or not to use or disclose the consumer's sensitive personal information for advertising and marketing. *Supra* note 63.

[72] Personal Information Protection Law of the People's Republic of China, 30th meeting of the Standing Committee of the National People's Congress of the People's Republic of China (NCP) on Aug 20, 2021, (https://personalinformationprotectionlaw.com/) (accessed 17th July, 2024).

[73] Anna Gamvros and Ruby Kwo, "China propose to ease cross border data transfer restrictions", Data Protection Report, Data Protection Legal insight at the speed of technology Oct 20, 2023, https://www.dataprotectionreport.com/2023/10/china-proposes-to-ease-cross-border-data-transfer-restrictions/#:~:text=Currently%2C%20the%20PIPL%20requires%20that,was%2028%20February%202023)%3B, (accessed 21st July, 2024).

[74] Gabriela Kennedy and Joshua T K Woo, "China Proposes Easing of Cross-Border Data Controls", Mayer Brown, Oct 11, 2023, (https://www.mayerbrown.com/en/perspectives-events/publications/2023/10/china-proposes-easing-of-cross-border-data-controls) (accessed 16th July, 2024).

[75] Ting Zheng and Ziyan "Fran" Xue, "Cross- Border Data Transfer Under Chain's Personal Information Protection Law", Womble Bond Dickinson, May 31, 2023, (https://www.womblebonddickinson.com/us/insights/blogs/cross-border-data-transfers-under-chinas-personal-information-protection-law), (accessed 27th July 2024).

Journal of Information Systems Engineering and Management
2025, 10(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

of the recipient to protect the data. These agreements are intended to guarantee that the personal information of individuals is not misused or improperly handled during cross-border transfers. The major article of China Personal Information Protection Law that deals with cross-border data transfer are Article 38,[76] which discusses the essential criteria for cross-border data transfer, and Article 39[77] ***"intimation to individuals for cross-border data transfer and separate consent from the individual",***
Article 40[78] ***"Security assessment by the National Cyberspace Department"*** and Article 42[79] of Personal Information Protection Law discuss the power of the National Cyberspace Department to limit the sharing of data to any country and can list it as a prohibited recipient of personal information. The provisions relating to cross-border data transfers under the China PIPL are comprehensive and rigorous, aiming to ensure the security and protection of personal information during international transfers[80]. The requirements for security assessments, regulatory approvals, and guarantees from overseas recipients demonstrate PIPL's commitment to safeguarding the privacy and rights of individuals in the digital age.

Furthermore, the Personal Information Protection Law imposes strict requirements on cross-border data transfers. Article 40[81] of the PIPL states that the data transfer outside of China must be in conformity with the requirements established by the Cyberspace Administration of China (CAC) or other relevant authorities. This

[76] Personal Information Protection Law of the People's Republic of China 2021, Article 38- A personal information processor that truly needs to provide personal information for a party outside the territory of the People's Republic of China for business sake or other reasons, shall meet one of the following requirements:
(1) Passing the security assessment organized by the national cyberspace department in accordance with Article 40 of this Law;
(2) obtaining personal information protection certification from the relevant specialized institution according to the provisions issued by the national cyberspace department.
(3) concluding a contract stipulating both parties' rights and obligations with the overseas recipient in accordance with the standard contract formulated by the national cyberspace department, and
(4) meeting other conditions set forth by laws and administrative regulations and by the national cyberspace department.
Where an international treaty or agreement that the People's Republic of China has concluded or acceded to stipulated conditions for providing personal information for a party outside the territory of the People's Republic of China, such stipulation may be followed.
The personal information processor shall take necessary measures to ensure that the personal information processing activities of the overseas recipient meet the personal information protection standards set forth in this Law. *Supra* note 72.
[77] Personal Information Protection Law of the People's Republic of China 2021, Article 39-Where a personal information processor provides personal information for any party outside the territory of the People's Republic of China, the processor shall inform the individuals of the overseas recipient name and contact information, the purpose and means of processing, the categories of personal information to be processed, as well as the method and procedures for the individuals to exercise their rights as provided in this aw over the overseas recipient etc., and shall obtain individual's consent. *Supra* note 72.
[78] Personal Information Protection Law of the People's Republic of China 2021, Article 40-Critical information infrastructure operators and the personal information processors that process personal information up to the amount prescribed by the national cyberspace department shall store domestically the personal information collected and generated within the territory of the People's Republic of China. Where it is truly necessary to provide the information for a party outside the territory of the People's Republic of China, the matter shall be subjected to security assessment organized by the national cyberspace department. Where laws, administrative regulations, or the provisions issued by the national cyberspace department provide that security assessment is not necessary, such provisions shall prevail. *Supra* note 72.
[79] Personal Information Protection Law of the People's Republic of China 2021, Article 42-Where overseas organizations or individuals engage in personal information processing activities, which infringes upon the rights and interests of citizens of the People's Republic of China on personal information or endanger the national security or public interests of the People's Republic of China, the national cyberspace department may include them in a list of restricted or prohibited recipients of personal information, publicize the list, and take measures such as restricting or prohibiting the provisions of personal information for such organization and individuals. *Supra* note 72.
[80] Richard Mazzochi, Minny Siu, Andrew Fei, Yu Leimin and Luan Jianqi, "Cross-Border Data Transfer in China: CAC Proposes important Regulatory Relaxations", King & Wood Mallesons, Oct 18, 2023, (https://www.kwm.com/global/en/insights/latest-thinking/cross-border-data-transfers-in-china-cac-proposes-important-regulatory-relaxations.html) (accessed 25th July 2024).
[81] *Supra* note 78.

Journal of Information Systems Engineering and Management
2025, 10(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

means that companies and organizations transferring personal data across borders must obtain prior approval from the authorities and adhere to well-defined regulations and standards set by the CAC.

Personal Information Protection Law requires organizations to conduct a security assessment before transferring personal information overseas. This assessment aims to verify that the data transfer does not compromise the security and integrity of the data and that appropriate preventive measures are in place to protect the data during the transfer process. In contrast, the Digital Personal Data Protection Act focuses more on the rights of individuals and the obligations of organizations in handling and processing personal data. While it includes provisions for cross-border data transfers, they are not as comprehensive and detailed as those in the PIPL.

5.4. Canada: The Personal Information Protection and Electronic Documents Act 2000[82]

The Personal Information Protection and Electronic Documents Act (PIPEDA) is a crucial piece of legislation in Canada that governs the private sector's data handling process (the collection, use, and disclosure of personal information). However, PIPEDA does not prohibit personnel transfer to other jurisdictions like the EU GDPR. It does not establish any rules governing cross-border data transfer. However, PIPEDA has guidelines relating to consent, collection of data, accountability of the organizations, limitations to collection, retention of data (use, disclosure and retention of information) and principles relating to safeguarding personal information[83]. Schedule 1 of the Personal Information Protection and Electronic Documents Act (PIPEDA)- sets out the ***"Principles for the National Standard of Canada Entitled Model Code for the Protection of Personal Information, CAN/CSA-Q830-96".*** Principle 1[84] imposes the responsibility of the organization to safeguard personal information under their control. Principle 4.1 talks about the accountability of the organizations that are dealing with personal information, and it proves some principles that an organization needs to follow for the processing of personal data. Principle 4.1.3[85] ensures that the organizations shall adopt contractual or other means to strengthen the data protection framework while transferring data to a third party[86]. When it comes to cross-border data transfer, PIPEDA requires that organizations guarantee an equal level of protection to the data that is being transferred outside of Canada as it would have if the information had remained within the country.

Principle 4.1.4[87] stipulates that an organization must use contractual or other measures to maintain an equal level of security while data is being processed by a third party. It also imposes liability on an organization for data under its control. Ensuring the protection of personal information during transfer to multiple jurisdictions

---

[82] Personal Information Protection and Electronic Documents Act, S.C 2000, c. 5, Assented to April 13, 2000, (https://laws-lois.justice.gc.ca/eng/acts/p-8.6/page-1.html#h-416885).

[83] DLA Piper, "Data Protection Laws of the World", Jan 26, 2023, (https://www.dlapiperdataprotection.com/index.html?t=transfer&c=CA#:~:text=Transferring%20personal%20information%20outside%20of,to%20access%20by%20foreign%20governments%2C) (accessed 25, July 2024).

[84] Personal Information Protection and Electronic Documents Act, S.C 2000, Principle 1- An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party. Office of the Privacy Commission of Canada, "Processing Personal Data Across Borders Guidelines", *Supra* note 82.

[85] Personal Information Protection and Electronic Documents Act, S.C 2000, Principle 4.1.3- An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party. *Supra* note 82.

[86] Office of the Privacy Commission of Canada, "Processing Personal Data Across Borders Guidelines", (https://www.priv.gc.ca/media/1992/gl_dab_090127_e.pdf) (accessed 22nd July 2024).

[87] Personal Information Protection and Electronic Documents Act, S.C 2000, Principle 4.1.4- Organizations shall implement policies and practices to give effect to the principles, including
(a) implementing procedures to protect personal information; (b) establishing procedures to receive and respond to complaints and inquiries; (c) training staff and communicating to staff information about the organization's policies and practices; and (d) developing information to explain the organization's policies and procedures. *Supra* note 82.

Journal of Information Systems Engineering and Management
2025, 10(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

with possibly disparate privacy laws and regulations is crucial[88]. This section highlights the importance of holding organizations liable for managing data regardless of the place where it is being filtered.

6. LEGAL IMPLICATIONS OF CROSS-BORDER DATA TRANSFER:

In India, the protection of personal data is governed by the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, which set out the essential conditions for handling the data (collection, storage, and transfer of personal data) by Indian entities. However, these rules do not specifically address the mechanism for the transfer of cross-border personal data, leading to uncertainty and gaps in the legal framework for regulating such transfers. The absence of comprehensive regulations has raised concerns about the adequacy of the protection afforded to individuals' privacy rights when their personal data is transferred outside India. India's efforts to establish an extensive data protection regime with the Digital Personal Data Protection Act 2023 present an opportunity to align with GDPR-like principles. India's diverse population and cultural nuances present significant challenges in implementing GDPR-like principles.

Under the DPDP Act, cross-border data transfer is allowed. However, section 16(1)[89] of the Act authorizes the central government to restrict cross-border data transfer to certain countries by process of notification, and section 16(2)[90] of the Act clarifies that any law parallel to the Act provides a level of data protection, and limitations on cross-border data transfer will prevail over the provisions of Digital Personal Data Protection Act 2023. Furthermore, section 17[91] of the Act provides exemptions from compliance under certain circumstances, such as in the case of a legal right or claim to ascertain the financial position of a defaulter, processing by a court or tribunal a contract entered with a foreign country. With the expansion of digital technology and the global nature of many industries, the need for companies to transfer data across international borders has become increasingly common[92]. The General Data Protection Regulation (GDPR) has set a global benchmark for data protection, influencing jurisdictions worldwide. The legal Implications of cross-

[88] Teresa Scassa, "Bill C-11's Treatment of Cross-Border Transfers of Personal Information, Office of the Privacy Commissioner of Canada, May 021, (accessed Dec 14, 2023, 10:00 P.M), (https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2021/tbdf_scassa_2105/).

[89] The Digital Personal Data Protection Act 2023 (No. 22 of 2023) Gazette of India, August 11, 2023, (https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf)

[90] Digital Personal Data Protection Act 2023, s 16(1)- The Central Government may, by notification, restrict the transfer of personal data by a Data Fiduciary for processing to such country or territory outside India as may be so notified; and
(2) Nothing contained in this section shall restrict the applicability of any law for the time being in force in India that provides for a higher degree of protection for or restriction on the transfer of personal data by Data Fiduciary outside India in relation to any personal data or Data Fiduciary or class thereof. *Supra* note 90.

[91] Digital Personal Data Protection Act 2023, s 17(1) The provisions of Chapter II, except sub-sections (1) and (5) of Section 8 and those of Chapter III and Section 16 shall not apply where- (a) the processing of personal data is necessary for enforcing any legal right or claim; (b) the processing of personal data by any court or tribunal or any other body in India which is entrusted by law with the performance of any judicial or quasi-judicial or regulatory or supervisory function, where such processing is necessary for the performance of such function; (c) personal data is processed in the interest of prevention, detention, investigation or prosecution of any offence or contravention of any law for the time being in force in India; (d) personal data of Data Principal not within the territory of India is processed pursuant to any contract entered into with any person outside the territory of India by any person based in India;
(e) the processing is necessary for a scheme of compromise or arrangement or merger or amalgamation of two companies or a reconstruction by way of demerger or otherwise of a company, or transfer of undertaking of one or more company to another company, or involving division of one or more companies, approved by a court or tribunal or other authority competent to do so by law for the time being in force; and
(f) the processing is for the purpose of ascertaining the financial information and assets and liabilities of any person who has defaulted in payment due on account of a loan or advance taken from a financial institution, subject to such processing being in accordance with the provisions regarding disclosure of information or data in any other law for the time being in force. *Supra* note 90.

[92] Joshua P Meltzer and Peter Lovelock, "Regulating for a Digital Economy: Understanding the Importance of Cross-Border Data Flows in Asia", Brookings Blog March 20, 2018, (https://www.brookings.edu/articles/regulating-for-a-digital-economy-understanding-the-importance-of-cross-border-data-flows-in-asia/) (accessed 26th July 2024).

border data transfer under India's data protection regime focus on aspects such as data localization, transfer mechanism, regulatory oversight, and potential exceptions.

1. Data Localization:

Data localization refers to the practice of requiring that certain types of data be stored within a territory of a specific country[93]. Such restrictions mandate that personal information must be kept within restricted geographical areas to ensure that data remains subject to the laws and regulations of that jurisdiction. Secondly, it enhances data sovereignty, giving citizens control over personal data. Thirdly, the government may implement data localization requirements as part of cross-border data transfer and privacy regulation. Lastly, it serves as a measure for national security concerns; by keeping sensitive personal data within the territory, the government can better safeguard against unauthorized access to sensitive personal data.
Data localization requirements significantly impact cross-border data transfer activities. Establishing a local data centre modifies data processing practices and adheres to data protection regulations[94]. However, the Digital Personal Data Protection Act does not provide any requirement for data localization. The act should strengthen the security requirements for storing and processing personal data. There should be strict protocols for the encryption of data, limitations on access, and data retention periods to confirm that personal data is protected from potential data breaches and unauthorized access. Additionally, there should be requirements for regular security audits and assessments to verify conformity with the act and identify any potential vulnerabilities in the data protection measures.

2. Data Transfer Mechanism:

There should be some specific mechanism for organizations who are engaged in cross-border data transfer while ensuring data protection[95]. These mechanisms may include standard contractual clauses and adopt other approved safeguard measures. The Digital Personal Data Protection Act 2023 allows data transfer but does not have any standard data transfer guidelines which need to be incorporated into the data transfer mechanism. Striking the right balance is crucial to prevent misuse of personal data for surveillance while ensuring the nation's security. A lack of clarity in this regard may lead to legal and ethical dilemmas. One of the key legal implications of cross-border data transfer under the new Indian data protection regime requires that the recipient country should ensure compliance with a data transfer mechanism. Aligning India's data protection laws on data transfer mechanisms with EU GDPR can facilitate international data flow. Harmonizing data protection standards enhances cross-border data transfers, benefiting international trade and collaboration.

7. CONCLUSION

In conclusion, the Indian data protection regime presents a complex and evolving landscape for the transfer of cross-border data. The recent changes in the data protection framework through the Digital Personal Data Protection Act 2023 and the evolving regulatory frameworks have brought significant challenges and opportunities for cross-border data transfers. The current legal structure does not adequately address the challenges posed by cross-border data transfers and the implications for data protection and privacy. The strict restrictions on cross-border data transfers have raised concerns among businesses and international organizations that rely on the free flow of data across borders for their operations. There is an urgency to find a midway between protecting personal data and enabling the seamless sharing of data for legitimate purposes such as global business operations, research, and innovation.

---

[93] Richard D Taylor, "Data Localization: The Internet in the Balance", Telecommunications Policy, Volume 44, Issue 8, September 2010, 102003, DOI: https://doi.org/10.1016/j.telpol.2020.102003, (https://www.sciencedirect.com/science/article/abs/pii/S0308596120300951) (accessed 22nd July 2023).
[94] Vidhya Praveen Shetty and Dr Harunrashid A Kadri, "Significance of Data Localization in Data Protection – An Analysis", European Chemical Bulletin (EBC) ISSN 2063-5346, (https://www.eurchembull.com/uploads/paper/8842812bb14d1173aa43830dcee8b301.pdf)(accessed 25 July 2024).
[95] Bojana Bellamy and Markus Heyder, "Essentials Legislative Approaches for Enabling Cross-Border Data Transfer in a Global Economy", Centre for Information Policy Leadership White Paper (Hunton & Williams LLP) September 25, 2017, (https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper__final__-_essential_legislative_approaches_for_enabling_cross-border_data_transfers.pdf) (accessed 25th July 2024).

Journal of Information Systems Engineering and Management
2025, 10(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Additionally, the lack of a comprehensive legal framework for cross-border data transfer in India poses challenges for businesses and organizations. There is a need for clear guidelines and mechanisms to ensure that cross-border data transfers are permitted as per the guidelines and do not infringe upon individuals' privacy rights. The absence of a specific provision in the Digital Personal Data Protection Act, 2023 addressing cross-border data transfer adds to the ambiguity and uncertainty surrounding this issue. The Cross-border data transfer under the Indian data protection regime requires careful consideration of the legal requirements, regulatory compliance, and the ongoing changes in the global data protection landscape.