DATA PROTECTION AND CROSS-BORDER DATA TRANSFER

Priyadharsani Indra R, Vinayaka Mission's Law School

ABSTRACT

India's Digital Personal Data Protection Act, 2023 (DPDPA), along with the proposed rules for 2025, is the country's first complete law to protect personal data and regulate how data can be shared with other countries. Under Section 16 of the Act, personal data can usually be transferred outside India unless the Central Government specifically restricts certain countries or entities. This means India follows a more open system, where transfers are allowed unless they are clearly blocked. The draft rules give more clarity, especially for organizations known as Significant Data Fiduciaries (SDFs). These are large or important data handlers. The government, with the help of experts, can identify certain types of sensitive personal data that need stronger protection. For such data, SDFs may have to take permission before sending it abroad or ensure that foreign governments cannot easily access it.

Even though the law generally allows data to move freely, some sectors still follow stricter rules. For example, the Reserve Bank of India[1] requires payment data to be stored within India, and the Insurance Regulatory and Development Authority has similar rules for insurance data. This creates a mixed system, where some data can move freely while some must stay within the country.

This approach creates a few challenges. It may be difficult for businesses to clearly understand and follow the rules. It could also affect innovation and increase compliance costs. Compared to the European Union's GDPR, which uses clear standards and structured methods for data transfers, India's system gives more power to the government to decide.

As India moves towards full implementation of the law, it is important to maintain a balance. The country must protect people's privacy and national interests while also supporting business growth and technology development. Clear rules, transparency in decisions, and better guidance on international data transfers will help reduce confusion and support smooth global data flow.

[1] Reserve Bank of India, Storage of Payment System Data, RBI/2017-18/153, https://www.rbi.org.in (last visited Apr. 6, 2026).

INTRODUCTION

India's approach to data protection is changing as the country tries to balance two important goals: protecting personal data and allowing data to move across borders. The Digital Personal Data Protection Act, 2023 (DPDPA),[2]along with the Draft Rules of 2025, creates a new and developing legal system for this purpose. Under this law, a Data Fiduciary is any person or organization that decides why and how personal data is used.

According to the Draft Rules, especially Rule 14, any organization that processes personal data in India, or outside India while offering goods or services to people in India, can transfer that data to another country. However, this is allowed only if the transfer follows the restrictions set by the Central Government. When this rule is read together with Rule 12(4), it creates some confusion. Businesses may find it difficult to clearly understand what is allowed and what is not, which can affect their planning and operations. It may also create challenges for global data sharing.

Although the DPDPA 2023 seemed to support a flexible system where data transfers are generally allowed unless restricted, the Draft Rules appear to bring in stricter conditions in some cases. This is especially true for Significant Data Fiduciaries (SDFs), which are large organizations handling large amounts of data. These unclear and stricter requirements may reduce innovation, increase compliance burden, and create uncertainty for businesses.

When compared to the European Union's GDPR, which provides clear methods for transferring data, India's approach seems less defined. This shows the need for clearer rules and better guidance. India needs a balanced system that protects national interests and personal privacy, while also supporting business growth and participation in the global digital economy.

This paper will first look at how India's data localization policies have developed over time, moving from strict rules to a more flexible approach. It will then examine the issues and uncertainties in the Draft Rules, especially Rule 12(4), and how they affect Significant Data Fiduciaries. After that, it will compare India's system with the GDPR. Finally, it will discuss the challenges for social media companies and AI development, and suggest ways to create a

[2] The Digital Personal Data Protection Act, 2023, No. 22 of 2023, India Code (2023), https://egazette.gov.in (last visited Apr. 6, 2026).

clearer and more effective legal framework.

Regulatory Evolution of Data Localization Requirements

Data localization means rules that require data to be stored or processed within a country's borders. In simple terms, it limits how data can move from one country to another. These rules can be very strict, like completely banning data transfers outside the country, or more flexible, where data can be transferred only if certain conditions are met, such as getting user consent or ensuring that the receiving country has proper data protection laws.

India's approach to data localization has changed over time. The government has tried to balance three main goals: national security, economic growth, and participation in the global digital economy. In 2018, the draft Personal Data Protection Bill[3], based on the Srikrishna Committee report,[4] Introduced very strict rules. It required companies to store a copy of all personal data in India and stated that certain "critical personal data" must be stored and processed only within the country. The 2019 version continued these strict requirements, which raised concerns among businesses about high costs, practical difficulties, and negative effects on innovation and international trade.

Later, India started moving towards a more flexible system. The 2022 draft introduced a "whitelist" approach, where data could be transferred only to countries approved by the government. Finally, the Digital Personal Data Protection Act, 2023 adopted a more open "blacklist" system. Under this, data transfers are generally allowed unless the government specifically restricts certain countries.[4]

However, even though the DPDPA seems more flexible, the Draft Rules bring back some complexity. This is especially true for Significant Data Fiduciaries (SDFs), which are large organizations handling important or sensitive data. Under Rule 12(4), these entities may be required to follow stricter rules for certain types of personal data. They may not be allowed to transfer such data outside India without prior approval from the government. This creates a form of conditional data localization, even within a system that is supposed to allow free data

[3] Personal Data Protection Bill, 2019, Bill No. 373 of 2019, https://prsindia.org (last visited Apr. 6, 2026). [4] Justice B.N. Srikrishna Committee, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (2018), https://meity.gov.in (last visited Apr. 6, 2026).
[4] Personal Data Protection Bill, 2022 (Draft), Ministry of Electronics and Information Technology, https://www.meity.gov.in (last visited Apr. 6, 2026).

flow.

Another issue is the lack of clear guidelines. There is no detailed explanation of how organizations will be classified as SDFs or which types of data will face restrictions. This creates uncertainty for businesses, as they may not know in advance whether these rules will apply to them. As a result, companies may face difficulties in planning, compliance, and international operations.

The DPDP Act generally allows personal data to be transferred outside India. It only restricts transfers to certain countries that the government considers unsafe. This shows that the law supports free flow of data, with some limits for protection.

However, the Draft Rules make the system more complicated. They allow the government to identify certain types of personal data that cannot be transferred outside India at all, especially by large organizations called Significant Data Fiduciaries (SDFs). These types of data may include sensitive information like health or biometric data, but the rules are not very clear about this. Even if another country has strong data protection, these data categories may still not be allowed to leave India.

This approach is seen as a step backward because it limits global data flow. Today, many businesses depend on international data transfers for services like cloud storage, analytics, and artificial intelligence. Strict restrictions can increase costs, create operational difficulties, and slow down innovation. It may also isolate parts of India's digital economy from the global market.

Another issue is that these rules do not clearly improve data security. The original aim of the DPDP Act was to block data transfers only to risky countries. But now, the focus seems to be shifting towards restricting certain types of data in general, which may not always be necessary. There is also a lack of clarity about how the government will decide which data categories should be restricted. Terms like "traffic data" are not clearly explained, which creates confusion and makes compliance harder for businesses.

Rule 14 adds to this concern. It gives the Central Government wide powers to impose restrictions on data transfers through notifications. This means that even if the law appears flexible, the government can still introduce strong localization requirements at any time. In

practice, this could lead to a system where most data is forced to remain within India.

Instead of creating unclear and scattered rules, the law should clearly define the limits of government power. This will help protect individuals' data while also giving businesses better clarity and confidence.

At the same time, some level of data localization can be useful. Keeping sensitive data within India may help in law enforcement, reduce risks from foreign surveillance, and provide better control in a fast-changing technological environment.

Comparative Analysis

Different countries follow different approaches to data localization based on their own priorities. There is no single global system. For example, countries like China and Russia follow very strict data localization rules. They require most data to be stored within their borders to ensure strong government control and national security.

On the other hand, the European Union follows a different model through the General Data Protection Regulation (GDPR).[5] It does not directly force companies to store data only within Europe, but it sets strict conditions for transferring data outside the EU. These conditions indirectly encourage companies to keep data within the EU to avoid legal complications. This approach focuses more on protecting the rights of individuals rather than strict control.

India should try to find a balanced approach. Instead of imposing very strict rules, it should protect national interests while also allowing businesses to operate smoothly in the global digital market. This idea is also supported by India's Data Empowerment and Protection Architecture, which focuses on using data in a way that benefits both individuals and businesses.

RISKS AND CHALLENGES

Impact on Social Media Intermediaries

The current system raises several important concerns. First, with the rapid growth of artificial

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation), 2016 O.J. (L 119) 1, https://eur-lex.europa.eu (last visited Apr. 6, 2026).

intelligence and digital technologies, it is unclear how much control can be placed on cross-border data transfers without slowing down innovation. Too many restrictions may affect technological development. Second, there is confusion about how the law applies. It is not always clear whether the same rules apply to all organizations or whether different rules apply to government bodies and private companies. This lack of clarity makes it difficult to properly implement and follow the law. One major issue is the impact on social media companies. If these platforms are classified as Significant Data Fiduciaries (SDFs), they will have to follow strict rules. These may include storing data within India, using strong encryption, and limiting access to data.

For many social media companies, this can be difficult because they operate globally and depend on international data systems. Setting up data storage within India and changing their systems can be costly and time-consuming.

The rules also give the government the power to require certain types of personal data to be stored only in India. This means companies may need to invest heavily in local infrastructure and change their business models.

In addition, restrictions on transferring data across borders can create legal problems for multinational companies. Social media platforms may find it hard to follow Indian laws while also meeting the legal requirements of other countries where they operate.

Ambiguity in Defining Restrictions under Rule 14

Rule 14 gives the Central Government the power to place “restrictions” on transferring data outside India. However, the rule does not clearly explain how these restrictions will be decided. This lack of clear guidelines creates confusion and gives the government wide discretion, which may lead to inconsistent or even unfair decisions. For businesses, especially in sectors like technology, e-commerce, and fintech, this uncertainty creates serious problems. Companies may find it difficult to plan their operations because they do not know when or how restrictions may be applied. This can slow down their work, increase compliance costs, and reduce opportunities for global partnerships and innovation.

There is also a concern that these powers could be used for reasons beyond data protection. For example, restrictions might be used to support local industries or limit foreign competition. If

this happens, it could harm India's reputation in the global digital market. Such uncertainty may also discourage foreign companies from investing in India. Sectors like IT, fintech, and e-commerce depend heavily on the free flow of data across borders. If rules are unclear or unpredictable, companies may hesitate to expand their operations in India.

To solve these issues, the law should clearly define when and how restrictions can be applied. The government can set objective standards, such as checking whether the receiving country has strong data protection laws, considering how sensitive the data is, and ensuring that companies follow proper safety measures. Clear rules will help protect data while also supporting business growth and international cooperation.

The "Onward Transfer" Gap

India allows personal data to be transferred to other countries. However, the law does not clearly control what happens after the data reaches that country. For example, if data is sent from India to another country that is considered safe, the transfer is allowed. But if that country later shares the same data with another country or company, Indian law does not clearly regulate this second transfer. This creates a gap in data protection.

In comparison, the European Union's GDPR has clear rules for such situations. It ensures that once data is transferred, the same level of protection continues even in further transfers. The idea is that data should remain safe no matter where it goes. The GDPR follows two main methods to protect data. First, it checks whether the country receiving the data has strong data protection laws similar to those in the EU. Second, if such laws are not present, companies must use safeguards like legal agreements and ensure that individuals can take action if their rights are violated. To support this, the GDPR provides tools such as standard contracts and internal company rules.

Similarly, countries like Singapore also allow data transfers only when there is proper protection. This may be done through contracts or by taking user consent. India's current system is more limited in this area. While it allows cross-border data transfers, it does not clearly ensure protection after the data leaves the country. This shows the need for stronger rules.

India should create a clear system to regulate onward transfers. It should ensure that data

remains protected even after it is transferred to another country. This can be done by setting clear standards, requiring safeguards, and checking whether further transfers are safe. At the same time, India should design these rules based on its own needs. It should consider its technological capacity, support growth of its digital economy, and reduce risks like misuse of data by foreign entities. A stronger and clearer framework will help protect personal data while also supporting safe global data sharing. Comparison with Global Data Protection Laws

India's DPDP Act follows a more flexible but government-controlled approach when it comes to transferring data across borders. Under this law, the government has the power to decide which countries are not safe for data transfers. Data can be sent outside India unless a country is placed on this restricted list. In comparison, the European Union's GDPR follows a different method. It uses clear systems like standard contracts, company rules, and approval of safe countries to manage data transfers. This approach focuses more on risk assessment and allows companies to take responsibility for protecting data.

Because of this, the GDPR gives businesses more flexibility. Companies can create their own systems, as long as they meet legal standards. On the other hand, the DPDP Act gives more power to the Central Government, which means businesses have less control over how they manage international data transfers. Even with these differences, India's law shares some common goals with global data protection laws. Like the GDPR and the California Consumer Privacy Act (CCPA),[6] it aims to protect personal data, ensure transparency, and make organizations responsible for how they use data.

However, India's approach is more centralized, while laws like the GDPR allow a more business-driven system. As India continues to develop its data protection rules, it is important to maintain a balance. The country should protect privacy and national interests while also supporting businesses that depend on global data flows.

Compliance Strategies for Businesses

To follow the Digital Personal Data Protection (DPDP) Act, businesses need to take a clear and organized approach, especially when transferring data outside India.

[6] California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 et seq., https://leginfo.legislature.ca.gov (last visited Apr. 6, 2026).

Understanding Data Flow First, companies should clearly identify where personal data is stored and processed. This includes data shared with vendors, cloud service providers, and other third parties located outside India. Knowing this helps businesses understand their risks and responsibilities.

Staying Updated with Rules Businesses must regularly check for updates from the government. This includes knowing which countries are restricted for data transfers and any special rules for certain sectors. Staying informed helps avoid legal issues.

Improving Compliance Measures

Using Contracts for Protection

Companies should use proper agreements when transferring data abroad. These contracts should ensure that the data is protected even after it leaves India, similar to international practices.

Planning for Data Localization

In some cases, businesses may need to store data within India. For this, they can invest in local data centers or use a mix of local and global storage systems. This helps them follow the law while still working efficiently.

Engaging with Authorities

It is important for businesses to stay in touch with regulators and government bodies. This helps them understand new rules clearly and avoid mistakes in compliance.

By following these steps, businesses can manage cross-border data transfers more effectively while continuing their operations without major disruptions.

Artificial Intelligence (AI) Compliance with Localization Mandate

Artificial intelligence (AI) makes data protection more complex. AI systems need large amounts of data from different countries to work properly. They learn and improve by using diverse datasets. If strict data localization rules are applied, it may limit access to global data. This can reduce the quality and accuracy of AI systems. In important areas like fintech,

healthcare, and cyber security, AI depends on data from different regions. If data is restricted within one country, the results may become less reliable or biased.

Also, many AI companies use cloud systems that process data across multiple countries at the same time. If they are forced to store data only within India, it can increase costs, slow down operations, and make systems less efficient. It may also reduce opportunities for global collaboration.

While it is important to protect sensitive data, too many restrictions can slow down innovation. India should be careful to avoid rules that may affect its growth as a global leader in digital technology.

Recommendations

Rule 14 of the Draft DPDP Rules gives the government the power to control cross-border data transfers, but it does not clearly explain how this power will be used. This creates uncertainty for both businesses and individuals. To improve the system, Rule 14 should clearly allow data transfers when companies follow proper safety measures. These may include using strong contracts, internal company rules, or other legal methods that ensure data is protected even after it is transferred.

Restrictions should be applied only in serious situations. For example, data transfers can be limited when the receiving country has weak data protection laws or poses a high risk to privacy. These countries can be clearly listed by the government. This approach will help Indian businesses operate globally without unnecessary difficulties. At the same time, it will ensure that personal data remains protected in risky situations. A clear and balanced system will support both privacy and economic growth.

Bullet Dodged: Initial DPDP Law on Cross-Border Transfers

The earlier versions of the DPDP Bill had very strict rules for transferring data outside India. These rules were detailed and applied differently to various types of personal data. One important rule was related to sensitive personal data.[7]Companies were required to keep a copy of such data within India, even if they transferred it to another country. This means that data

[7] Monetary Authority of Singapore, Advisory Guidelines on the Personal Data Protection Act, https://www.mas.gov.sg (last visited Apr. 6, 2026).

could not be stored only abroad; it had to be stored in India as well. This requirement would have created major challenges for businesses. Companies, especially large international technology firms, would need to build or invest in data storage systems within India. This would increase costs and create operational difficulties. For example, a global company might already have data centers in different parts of the world. If it is forced to store the same data again in India, it would have to spend more money, manage additional systems, and handle more complex operations. Because of these challenges, such strict rules were seen as difficult to implement. Moving away from these heavy requirements has helped create a more flexible system under the current law.

Requirements for Cross-Border Transfers:

The 2019 draft further imposed specific obligations for transferring sensitive personal data internationally:

- Explicit consent from the data principal was mandatory.
- Where transfers were based on contracts or intra-group arrangements, such mechanisms required approval from the Data Protection Authority (DPA) in consultation with the Central Government.
- An adequacy assessment by the Central Government was necessary to ensure that the data would not be disclosed to foreign governments or agencies without authorization; alternatively, transfers could proceed with specific approval from both the DPA and the Central Government.

Restrictions on Transfer of Critical Personal Data: More stringent still was the near-prohibition on transferring critical personal data outside India. Additionally, subject only to narrow exceptions. Such data could be transferred in emergency situations or to specifically authorized entities compliance. In particular, transfers were permitted for immediate response scenarios, such as sharing data with entities involved in healthcare or emergency response services. Transfers to jurisdictions, entities, or international bodies recognized through a government-led adequacy determination as meeting national security safeguards.

Currently, it appears that restrictions on cross-border transfers of personal data have been delegated to subordinate rules under the Act, as well as to sector-specific regulators. This aspect

is explored further in subsequent sections. Ban on Blacklisted Territories. Cross-border transfers will be permitted to every country EXCEPT those specifically placed on a government-issued blacklist .The final version of the DPDP Act appears to follow a blacklist model, permitting data transfers to all countries EXCEPT the jurisdictions expressly restricted by the government. Put differently, personal data may be transferred to any nation except those identified on the government blacklist.

Take a multinational company operating in India that needs to send customer data to its analytics hub in Singapore. Under the DPDP Act, provided Singapore is not included on the blacklist, such a transfer is allowed.

A major loophole may emerge where data transferred to an approved country is later routed to a blacklisted jurisdiction. This may effectively defeat the protective objective of the Act unless addressed through future regulatory safeguards.

Sector-Specific Laws

The DPDP Act clearly states that if any other law in India provides stricter rules for data protection or cross-border transfers, those rules will apply instead of the DPDP Act. This means some sectors follow tougher data localization requirements. In the banking and payment sector, the Reserve Bank of India (RBI) has strict rules. According to its 2018 circular, all payment system data must be stored only within India. This includes customer details, transaction data, and payment-related information. However, if a transaction involves another country, the data may also be stored there if needed.

For non-banking financial companies (NBFCs), RBI guidelines require[8] that important records related to outsourced services must be kept in India. They also ensure that foreign regulators cannot access Indian data just because it is processed outside the country. In the insurance sector, the Insurance Regulatory and Development Authority of India (IRDAI) requires that all insurance records, such as policies and claims, must be stored within India. Even when companies outsource their work, original policyholder data must remain in India.

Similarly, the Securities and Exchange Board of India (SEBI) has rules for companies using

[8] OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2013), https://www.oecd.org (last visited Apr. 6, 2026).

cloud services. These rules require that all important data, including system logs, must be stored and processed within India. For foreign investors, their data must also be easily accessible within the country. Overall, these sector-specific laws create stricter data localization requirements in important industries. Even though the DPDP Act allows flexible data transfers, these additional rules make the system more complex for businesses to follow.

SEBI Advisory on SaaS-Based Solutions and Companies Act Requirements

The Securities and Exchange Board of India (SEBI) has issued guidelines for financial entities that use Software as a Service (SaaS) solutions. These include merchant bankers, credit rating agencies, depository participants, and other intermediaries. According to SEBI, such entities must store important data within India. This includes sensitive information like credit risk data, liquidity data, market risk data, system-related details, vendor information, audit records, and network design. The aim is to ensure that critical financial data remains under India's legal control and is easily accessible when required.

In addition to this, the Companies Act, 2013 also places requirements on companies. Under Section 128, every company must maintain its books of accounts and financial records at its registered office.

Further, an amendment made on 5 August 2022 states that if these records are stored electronically, they must always be accessible within India. This means that even if companies use digital systems or cloud storage, they must ensure that the data can be accessed from within the country at any time.

Together, these rules strengthen data localization in the financial and corporate sectors. They ensure better control, transparency, and regulatory access, but also add to compliance responsibilities for businesses. Additional Sector Rules and Practical Examples In the telecom sector, the Department of Telecommunications (DoT) has strict rules under the Unified License. It states that companies cannot transfer subscriber information or user data outside India. Only a few exceptions are allowed, such as international roaming or specific foreign subscriber services. The Ministry of Electronics and Information Technology (*Meit*)[9] also introduced Cyber Security Directions in 2022. These rules require service providers in India to

[9] NITI Aayog, Data Empowerment and Protection Architecture (DEPA), https://www.niti.gov.in (last visited Apr. 6, 2026).

store and maintain logs of financial transactions within the country. This helps in improving cyber security, monitoring activities, and responding quickly to cyber threats.

Similarly, under the Consumer Protection (Direct Selling) Rules, 2021, companies involved in direct selling must store sensitive personal data within India. This ensures better protection of consumer information.

Examples

To understand this better, consider a few examples:

If a bank like HSBC wants to improve its global data systems, it still has to follow RBI rules. Even if it uses international platforms, all payment-related data must be stored within India. This may require the bank to set up or use local data centers. In another example, if an insurance company like LIC works with a technology company to develop AI-based services, it must follow IRDAI rules. This means all policyholder and claims data must remain within India, even if global cloud services are more efficient.

These examples show that even if the DPDP Act allows data transfers, companies must still follow stricter sector-specific laws. If another law restricts data transfer, that restriction will apply. How Does the DPDP Compare with Other Data Protection Regimes The European Union's GDPR provides a clear and well-structured system for cross-border data transfers. Under the GDPR, data can be transferred to another country only if that country offers a similar level of data protection. The European Commission identifies such countries as "adequate."

If a country is not considered adequate, companies can still transfer data by using certain safeguards.

These include internal company rules or legal agreements that ensure the data remains protected even after transfer. These rules clearly explain how cross-border transfers should take place. In comparison, India's DPDP Act follows a different approach. It allows data transfers by default, unless the government specifically restricts certain countries. However, the Act does not clearly explain how these countries will be selected or what criteria will be used.

Also, unlike the GDPR, the DPDP Act does not require companies to prove that the receiving country has strong data protection laws. It also does not clearly require the use of safeguards

like contracts or internal company rules for such transfers.

Because of this, the DPDP system is more flexible but also less clear, which may create uncertainty for businesses.

How Can Businesses Prepare for Upcoming Changes?

Since the final DPDP Rules are not yet fully clear, businesses should start preparing in advance. First, companies should understand where their data is stored and processed, especially if it is located outside India. This includes checking their systems, vendors, and technology partners. Second, businesses should regularly follow government updates. They need to know if any countries are added to the blacklist or if new rules are introduced. Third, companies should check if they are subject to any sector-specific laws, as these may have stricter requirements than the DPDP Act. They should also be ready to adopt new compliance methods, such as using contracts or internal rules for safe data transfers, if required in the future.

Most importantly, businesses should begin by understanding the basics of the DPDP Act. This includes knowing its scope, exemptions, and penalties. Having a clear understanding will help them build a strong compliance system and avoid future risks

The GDPR provides clear systems to decide when cross-border data transfers are allowed. It uses three main methods: approved countries (adequacy decisions), standard contracts between companies, and internal company rules. These methods help ensure that personal data remains protected even when it is transferred to another country. In contrast, the DPDP Act does not clearly provide such systems. It does not require the government to define standards for data protection in other countries or to create clear rules like contracts or internal company policies for safe transfers. Because of this, businesses may need to depend on their own agreements and safeguards to protect data.

Another important issue is that the power to restrict countries is fully in the hands of the Central Government. This gives the government a lot of control, and there is a possibility that such decisions may be influenced by political or other non-legal factors.

Also, under Section 16(2) of the DPDP Act, sector-specific laws are given more importance. This means that if another law has stricter rules for data transfers, those rules will apply instead of the DPDP Act. As a result, different sectors may follow different standards.

At the same time, it is important to understand that not all data can be completely restricted in the name of privacy. Some sectors need to transfer data to function properly. However, since the law is still new and not fully implemented, its real impact is not yet clear. This uncertainty may affect how effective the law will be in practice

Therefore, there is a strong need for a clear and well-designed legal framework to manage cross-border data transfers. Data is often called the "new oil" because of its high value in today's digital world. It is important to protect this data, but at the same time, the law should not slow down economic growth.

Delays in implementing the Act and the existing gaps in rules for international data transfers create risks. Without proper safeguards, valuable data may be exposed to misuse or security threats. Hence, it is important for the government to take timely action and create clear rules that both protect data and support business and innovation

Conclusion

Cross-border data transfers can create serious risks if they are not properly controlled. Just like diseases can spread quickly, data risks can also move across countries if there are no strong protections. It is the responsibility of the government to create systems that can protect data from such risks. The current framework in India still has many unclear areas. There is confusion about how restrictions will be applied, lack of clear standards, and gaps in how data transfers are managed. These issues need to be fixed to make the system more reliable and effective. India needs clear and strong rules that both protect data and allow it to move safely across borders. This will help prevent data misuse, protect national security, and ensure that people's privacy is respected.

At the same time, the law should support the smooth flow of data for business and innovation. Privacy should not be treated as something optional. People should not have to give up their privacy just to use digital services. An important question still remains: is data fully protected when it is transferred outside

India. The answer is not yet clear. The government must address this concern by creating better safeguards and clearer rules. In the future, laws should focus not only on controlling data transfers but also on preventing misuse. Strong penalties should be applied to those who misuse

data or harm individuals through cyber activities. This will help protect people's right to privacy and build trust in the digital system.