



## NAVIGATING DATA SOVEREIGNTY: INDIA'S UNIQUE APPROACH TO DATA PROTECTION IN THE GDPR ERA

---

Aditi Sharma \*

### ABSTRACT

*While watching the developments of the new international data governance regime, the Indian model of data protection and privacy legislation and regulation is quite different from the GDPR model. This research examines India's unique regulatory position, focusing on three critical aspects: The key measures adopted by European countries include data localisation requirements, government access and cross-border data transfer standards. This work's comparative analysis of legislative texts, policy documents, and implementation examples shows how India's approach is based on digital sovereignty and national security to meet the country's economic development and international trade requirements. The outcomes demonstrated that a framework that is distinct in its approach from the GDPR is implemented in India to address the data localization issues of the country and due to the broader rights of the Indian government to access data because of security and economic objectives. On the one hand, this approach has led to the creation of national digital solutions and innovations; on the other hand, it has increased incomparable compliance obligations for international organisations and raised fundamental concerns regarding the attainment of GDPR adequacy. The research also establishes further implementation issues such as infrastructure development requirements, compliance expenses, and compatibility with global standards. These findings have significant implications for GDT as they show that India's model might be an inspiration for other emerging markets looking for a way to maintain their digital sovereignty while being connected to the global economy. This work adds to the emerging literature on critical perspectives on the data protection regulation and offers policy implications for decision makers and firms engaged in the global governance of data.*

---

\*ADVOCATE.

**Keywords:** Data Sovereignty, Data Localization, GDPR Compliance, Digital Privacy, Cross-Border Data Flows, Data Protection Framework, Digital Governance, Cybersecurity Policy, Data Residency Requirements, Privacy Regulations, Digital Economy, Information Technology Law, Data Processing, International Data Transfer, Regulatory Compliance, Digital Infrastructure, Government Data Access, Privacy Rights.

## INTRODUCTION

Modern society has become a digital society, which means that the protection of data and regulation of privacy have become an urgent issue, where countries have different approaches to the resolution of these problems. Although the EU's GDPR has become a powerful model for many countries, India decided to build a unique model that meets its specific needs as a rapidly developing digital economy with different security and economic priorities.<sup>1</sup>

## INDIA'S DISTINCTIVE APPROACH TO DATA PROTECTION

### Data Localization Requirements

Another essential feature of the Indian approach is to consider data localization as its major principle. Although the GDPR was supposed to ensure adequate protection irrespective of the location of the transfer, India has made a rule that some types of data must be processed within the country. This need is justified by several factors, including national security, the interests of law enforcement agencies as well and encouraging local players in the digital economy market.

The framework separates data into different classes, where each class has different localization rules. While the CPD data has to be stored and processed only in India, the SPD can be transferred to a country other than India only under circumstances. This tiered strategy is a high-wire act between protecting national data and the free flow of data across borders that business relies upon.<sup>2</sup>

---

<sup>1</sup> 'Key Global Takeaways from India's Revised Personal Data Protection Bill' (*Default2020*) <<https://www.lawfaremedia.org/article/key-global-takeaways-indias-revised-personal-data-protection-bill>> accessed 30 October 2024.

<sup>2</sup> DS\_MarkeTeam, 'Data Regulation - India - DS-Avocats' (*DS-Avocats* 12 February 2024) <<https://www.dsavocats.com/en/data-regulation-india/>> accessed 30 October 2024.

## **Government Access and National Security**

India's framework provides a broader list of situations than the GDPR and enables the government to engage with data. This approach is in compliance with the Indian government, emphasis on the internal security and policing needs in the modern technological age. Controlling the access to data is not excluded and the framework does include provisions for it under some circumstances, although the measures are quite different from the strict prohibits of the GDPR for state access. The rationale for these wider access provisions is sought in the peculiarities of the security situation in India and the necessity to secure effective policing in the context of the use of new technologies. Nonetheless, this approach has amplified several legal concerns with regard to the protection of state and personal data, especially in an international dimension.

## **Cross-Border Data Flows**

India's regime for cross-border transfer of data is a paradigm shift from the GDPR model, which has adequacy decisions or appropriate mechanisms for processing data across borders. India's approach, therefore, focuses on data nationalism with a view to enabling the necessary cross-border data flows.<sup>3</sup> Therefore, complex conditions have been defined for the cross-border transfers. These are requirements to keep a copy of the data within India, the obligation of the processor to seek prior regulatory authorization for some types of transfers, restrictions placed on transfers to certain foreign countries, and requirements concerning the data-sharing contracts. Such an approach develops a complex system of regulation for the purpose of achieving greater national interests against the background of existing commitments to exchange data globally.<sup>4</sup>

## **ECONOMIC AND TECHNOLOGICAL IMPLICATIONS**

### **Impact on India's Digital Economy**

The current approach to data protection in India has deep consequences for the country's domestic digital economy. While it may have implications of being a barrier to entry for certain

---

<sup>3</sup> Danielle Luo, 'In India, Data Protection Is Expanding State Power' (*Centre for International Governance Innovation* 2 October 2023) <<https://www.cigionline.org/articles/in-india-data-protection-is-expanding-state-power/>> accessed 30 October 2024.

<sup>4</sup> 'Transfer in India - DLA Piper Global Data Protection Laws of the World' (*Dlapiperdataprotection.com* 2018) <<https://www.dlapiperdataprotection.com/index.html?t=transfer&c=IN>> accessed 30 October 2024.

business entities, the data localization requirements are expected to create demand for local data centres and domestic technology development. This is in line with the general Indian economic plan of building digital self-sufficiency and encouraging domestic development.<sup>5</sup> The framework has already led to more investment in local data storage and processing centres. Large technology firms have disclosed intentions to set up or increase data centres in India, thus boosting the local digital infrastructure. This development is generating new opportunities for local commercial players as well as technology vendors while possibly decreasing dependence on cross-border digital infrastructure.<sup>6</sup>

### **International Business Operations**

The requirements of the framework present both risks and opportunities for international companies doing business in India. Some companies have to change the way in which they gather, manage, and process data to meet the requirements of localization, which usually requires significant investments in local infrastructure or cooperation with local suppliers. These adaptations have caused an increase in operational costs and require a change in the way data is processed. In order to operate successfully in the regulatory environments, firms are improving their domestic affiliations and capital expenditures. Also, there is clear evidence of the emergence of business models that are peculiar to the Indian market only. Consequently, it is in this light that companies endeavour to exploit new opportunities in addition to heeding the localization policies in India.

### **Innovation and Competitiveness**

These trends affect innovation and competitiveness in the digitized market of India with regard to data localization and sovereignty. While some scholars have argued that these requirements could prejudice international cooperation and the availability of world innovations on our territory, some international scholars are pinioned that, on the contrary, they can spur domestic innovations and non-dependence on foreign technologies.

---

<sup>5</sup> STL TECH, 'How Would Data Localization Benefit India?' (*STL Tech* 8 February 2023) <<https://stl.tech/blog/how-would-data-localization-benefit-india/>> accessed 30 October 2024.

<sup>6</sup> ET CIO, 'Data Localisation in India: Significance and Economic Impact' (*ETCIO.com* 13 August 2021) <<https://cio.economictimes.indiatimes.com/news/strategy-and-management/data-localisation-in-india-significance-and-economic-impact/85292096>> accessed 30 October 2024.

## CHALLENGES AND OPPORTUNITIES

### Implementation Challenges

Challenges for India's implementation of a data protection framework arise. Firstly, there is an urgent need to create, in the near future, enough technical base for data storage and processing domestically, which is a big problem. Secondly, compliance costs are raised by the need to spend a lot of money on new systems and processes to meet data localization requirements. Also, building local talent in data protection and privacy management is essential, something that requires sound skill development measures in place to guarantee sufficient data handling. Last but not least, while following localization norms, India needs to ensure cross-border data flow. This poses the need for synchronisation with global actors to allow smooth contactless communication and operation in the digital realm without negotiations of policy on privacy or periodic interferences to business. These challenges demonstrate that it is an uphill task to build a strong framework of data protection that addresses the domestic capacity as well as the international collaboration and conformity.

### Opportunities for Growth

Despite this, the framework presents various opportunities that would immensely benefit the domestic technology space. First, it can lead to the emergence of a strong domestic data centre industry, which is lacking at the moment and contributes to the development of the economy. This development continues to foster the growth of local technology services, allowing firms to provide a greater number of solutions that leverage innovative technologies to meet the requirements of the local market.<sup>7</sup> Furthermore, the framework improves cybersecurity since it promotes the use of local resources to address high risks of cybersecurity threats to sensitive data. It also leads to the localization of growth, which reduces reliance on external technologies and increases digital independence and control amongst nations. Consequently, all these factors are in synergy to foster a favourable climate for tech development and security for both the

---

<sup>7</sup> Zinnov, 'The Privacy Pivot: How Software & Internet GCCs Can Gear up for India's New Data Protection Era' (Zinnov13 September 2023) <<https://zinnov.com/centers-of-excellence/preparing-software-and-internet-gccs-for-indias-data-protection-era-blog/>> accessed 30 October 2024.

private and public domains to take advantage of digital levers for sustainable growth and improved national security.<sup>8</sup>

## CASE STUDIES AND IMPLEMENTATION EXAMPLES

### Impact on Global Digital Trade and Governance

India is also contributing to forming the rules and regulations of international data sharing with consequences for the architecture of the digital economy. Given that India is one of the biggest and fastest-growing digital economies, its regulatory position is quite influential. Its model of data localization requirements, the broad governmental access to data, and intricate preconditions for international data transfers might serve as a precedent for other EMs that look for an opportunity to strengthen their digital sovereignty. This could result in a world where there will be several disparate data management structures, displacing the present dominance of the Western model, such as the GDPR.<sup>9</sup>

The contradiction between India's internal policy considerations and the integrationist goals of international digital platforms shows that the formation of a coherent international digital system is problematic. India's experience shows that there is no easy way to balance the national interests with the requirements of the connected digital environment. This portends similar frictions as other players try to set rules for the global digital economy that they prefer for their own development and security.<sup>10</sup>

In the end, India's approach to data protection could become a model for how emerging markets are attempting to navigate between the imperative of asserting their digital sovereignty and the imperatives of global data flows. The international community will be closely observing how the Indian framework unfolds, as it may contain some lessons for the countries grappling with the question of how to pursue national interest while not disturbing international cooperation

---

<sup>8</sup> Express Computer, 'India's Data Protection Law: Reimagining a New Era of Innovation Led Digital Markets' (*Express Computer* 9 February 2024) <<https://www.expresscomputer.in/guest-blogs/indias-data-protection-law-reimagining-a-new-era-of-innovation-led-digital-markets/108959/>> accessed 30 October 2024.

<sup>9</sup> 'Understanding India's New Data Protection Law' (*Carnegie Endowment for International Peace* 2023) <<https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law?lang=en>> accessed 30 October 2024.

<sup>10</sup> 75, 'India - Digital Economy' (*International Trade Administration / Trade.gov* 18 September 2024) <<https://www.trade.gov/country-commercial-guides/india-digital-economy>> accessed 30 October 2024.

and integration. This has major implications for policymakers and businesses seeking to understand and participate in the complex world of global digital trade and regulation.<sup>11</sup>

### **WhatsApp's Data Localization Journey**

Perhaps the most famous example of how India's data protection laws are affecting foreign businesses is the case of WhatsApp. India required all payment data to be stored domestically in 2018, which became a problem for WhatsApp when it launched WhatsApp Pay, based on UPI.<sup>12</sup> Firstly, WhatsApp was slow to change because its data storage structure was implemented internationally. Nevertheless, by the year 2020 the company adapted itself by investing in Indian infrastructure as well as adopting certain particularities regarding data processing in the country.<sup>13</sup> These changes included establishing Payment servers in India for Payment data storage, developing Compliance monitoring systems, segregating Indian user data and developing Privacy features for India. This adaptation process shows the challenges and possibilities required by international firms in India's legal framework. However, due to the successful modifications, WhatsApp can continue funding its operations in India, one of the largest markets in the world.<sup>14</sup>

### **Domestic Innovation: Paytm's Data Infrastructure**

Paytm, the largest digital payment platform in India, is one of the tactics by which domestic actors capitalized on data localization requests strengthening their positions. Before the increase in stringent rules, the company strategically built strong local data structures. Paytm's plan was to have multiple data centres in India, build domestic data processing systems, implement privacy solutions in India, and establish security operational centres. Such initial steps have helped Paytm to maintain the competitive edge in front of international players who could not align their systems with India's rigid data localization policies.

---

<sup>11</sup> Arindrajit Basu, 'Sovereignty in a "Datafied" World' (*orfonline.org* 23 April 2023)

<<https://www.orfonline.org/research/sovereignty-in-a-datafied-world>> accessed 30 October 2024.

<sup>12</sup> Sankalp Phartiyal and Aditi Shah, 'WhatsApp Builds System to Comply with India's Payments Data Storage Norms' (*Reuters* 9 October 2018) <<https://www.reuters.com/article/us-india-payments-whatsapp/whatsapp-builds-system-to-comply-with-indias-payments-data-storage-norms-idUSKCN1MJ0IX/>> accessed 30 October 2024.

<sup>13</sup> Digbijay Mishra, 'NPCI Confirms WhatsApp Pay's Data Localisation' (*The Times of India* 28 July 2020) <<https://timesofindia.indiatimes.com/business/india-business/npci-confirms-whatsapp-pays-data-localisation/articleshow/77228456.cms>> accessed 30 October 2024.

<sup>14</sup> ET Bureau, 'WhatsApp Pay Has Now Met All Data Localisation Rules, NPCI Tells RBI' (*The Economic Times* 4 August 2020) <<https://economictimes.indiatimes.com/small-biz/startups/newsbuzz/whatsapp-pay-has-now-met-all-data-localisation-rules-npci-tells-rbi/articleshow/77343179.cms?from=mdr>> accessed 30 October 2024.

### **Cross-Border Challenges: TCS and International Client Data**

Tata Consultancy Services (TCS) – India’s largest IT services firm – is a case in point of managing cross-border data transfers under existing architectures. Operating in both Indian and international territories, TCS efficiently manages sensitive data through its complex system of compliance with both Indian and international privacy legislation. This implies separate processing environments for each jurisdiction as well as real-time tracking of data localization, automated compliance management system and data access controls to specific jurisdictions. The vast structure in TCS demonstrates how Indian corporations address domestic and global responsibilities, which incurred approximately \$250 million in compliance from 2019 to 2021, explaining the significant cost of such obligations for global business.

### **Government Implementation: Aadhaar Data Protection**

The Aadhaar biometric identification system of India reveals how the government departments change according to the contemporary data protection acts. UIDAI has put in place elaborate measures as follows: the biometric data is encrypted beyond the normal standard for data stored; several layers of authentication are required to access the data; periodic security reviews accompanied by vulnerability tests.<sup>15</sup> Moreover, there is a strict documentation of the Data Access Control, which ensures security in the information. This scenario points to what many government agencies have been able to strike between adequate data protection and legitimate access. Such endeavours tend to underscore the stance of preserving security to support functionality in essential identification systems.

### **CONCLUSION**

As the country implements new technologies, its sovereignty has to be maintained, but at the same time, the international standards have to be met. Economic competitiveness also has to be sustained in a digital economy. Measures that can be taken at the policy and corporate levels are modification of framework standards, elaboration of guidelines for the implementation process, strengthening of inter-country collaboration, and strengthening of industry-specific capacities. They are meant to maintain India’s data protection mechanisms functional while changes occur and to provide direction on data management. Strategic recommendations include the need to proactively plan compliance activities, develop local resources and

---

<sup>15</sup> JisaSoftech, ‘WHAT GOES into MAKING AADHAAR SAFE?’ (*JISA Softech Pvt Ltd* September 2022) <<https://www.jisasoftech.com/what-goes-into-making-aadhaar-safe/>> accessed 30 October 2024.

cooperation, plan for future modifications to data management and improve privacy and security. Therefore, the strategy of India covers Digital Governance issues and India's issues of security and economy, in one way or the other. Although distinct from the EU's GDPR due to India's global role, successful implementation necessitates balancing objectives: safeguarding individuals' information in the processing and sharing of information with the growth of the economy, strengthening the security of the state, and international data transfer. India's experience during the development of a proper data protection regime will be valuable for other countries aspiring to gain greater digital sovereignty. People of the world will watch India's framework development as how the country will preserve its own interests while pursuing integrationist objectives. The analysis suggests that there is a need for continuous research and study to appreciate India's international approach towards digital governance. Such knowledge will put policymakers and businesses in a better standing to address the data privacy issues that come with globalization.

## **BIBLIOGRAPHY**

- [1] 'Key Global Takeaways from India's Revised Personal Data Protection Bill' (Lawfare, 2020) <https://www.lawfaremedia.org/article/key-global-takeaways-indias-revised-personal-data-protection-bill> accessed 30 October 2024.
- [2] DS\_MarkeTeam, 'Data Regulation - India - DS-Avocats' (DS-Avocats, 12 February 2024) <https://www.dsavocats.com/en/data-regulation-india/> accessed 30 October 2024.
- [3] Danielle Luo, 'In India, Data Protection Is Expanding State Power' (Centre for International Governance Innovation, 2 October 2023) <https://www.cigionline.org/articles/in-india-data-protection-is-expanding-state-power/> accessed 30 October 2024.
- [4] 'Transfer in India - DLA Piper Global Data Protection Laws of the World' (Dlapiperdataprotection.com, 2018) <https://www.dlapiperdataprotection.com/index.html?t=transfer&c=IN> accessed 30 October 2024.
- [5] STL TECH, 'How Would Data Localization Benefit India?' (STL Tech, 8 February 2023) <https://stl.tech/blog/how-would-data-localization-benefit-india/> accessed 30 October 2024.

[6] ET CIO, 'Data Localisation in India: Significance and Economic Impact' (ETCIO.com, 13 August 2021) <https://cio.economicstimes.indiatimes.com/news/strategy-and-management/data-localisation-in-india-significance-and-economic-impact/85292096> accessed 30 October 2024.

[7] Zinnov, 'The Privacy Pivot: How Software & Internet GCCs Can Gear up for India's New Data Protection Era' (Zinnov, 13 September 2023) <https://zinnov.com/centers-of-excellence/preparing-software-and-internet-gccs-for-indias-data-protection-era-blog/> accessed 30 October 2024.

[8] Express Computer, 'India's Data Protection Law: Reimagining a New Era of Innovation Led Digital Markets' (Express Computer, 9 February 2024) <https://www.expresscomputer.in/guest-blogs/indias-data-protection-law-reimagining-a-new-era-of-innovation-led-digital-markets/108959/> accessed 30 October 2024.

[9] 'Understanding India's New Data Protection Law' (Carnegie Endowment for International Peace, 2023) <https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law?lang=en> accessed 30 October 2024.

[10] '75, 'India - Digital Economy' (International Trade Administration | Trade.gov, 18 September 2024) <https://www.trade.gov/country-commercial-guides/india-digital-economy> accessed 30 October 2024.

[11] Arindrajit Basu, 'Sovereignty in a "Datafied" World' (orfonline.org, 23 April 2023) <https://www.orfonline.org/research/sovereignty-in-a-datafied-world> accessed 30 October 2024.

[12] Sankalp Phartiyal and Aditi Shah, 'WhatsApp Builds System to Comply with India's Payments Data Storage Norms' (Reuters, 9 October 2018) <https://www.reuters.com/article/us-india-payments-whatsapp/whatsapp-builds-system-to-comply-with-indias-payments-data-storage-norms-idUSKCN1MJ0IX/> accessed 30 October 2024.

[13] Digbijay Mishra, 'NPCI Confirms WhatsApp Pay's Data Localisation' (The Times of India, 28 July 2020) <https://timesofindia.indiatimes.com/business/india-business/npci-confirms-whatsapp-pays-data-localisation/articleshow/77228456.cms> accessed 30 October 2024.

[14] ET Bureau, 'WhatsApp Pay Has Now Met All Data Localisation Rules, NPCI Tells RBI' (The Economic Times, 4 August 2020) <https://economictimes.indiatimes.com/small-biz/startups/newsbuzz/whatsapp-pay-has-now-met-all-data-localisation-rules-npci-tells-rbi/articleshow/77343179.cms?from=mdr> accessed 30 October 2024.

[15] JisaSoftech, 'WHAT GOES into MAKING AADHAAR SAFE?' (JISA Softech Pvt Ltd, September 2022) <https://www.jisasoftech.com/what-goes-into-making-aadhaar-safe/> accessed 30 October 2024.