# Regulatory Burden

## ON MICRO-SMALL AND MEDIUM BUSINESSES DUE TO DATA LOCALISATION POLICIES

Indian Council For Research On International Economic Relations

*September 2019*

DATA Catalyst

ICRIER

## TABLE OF CONTENTS

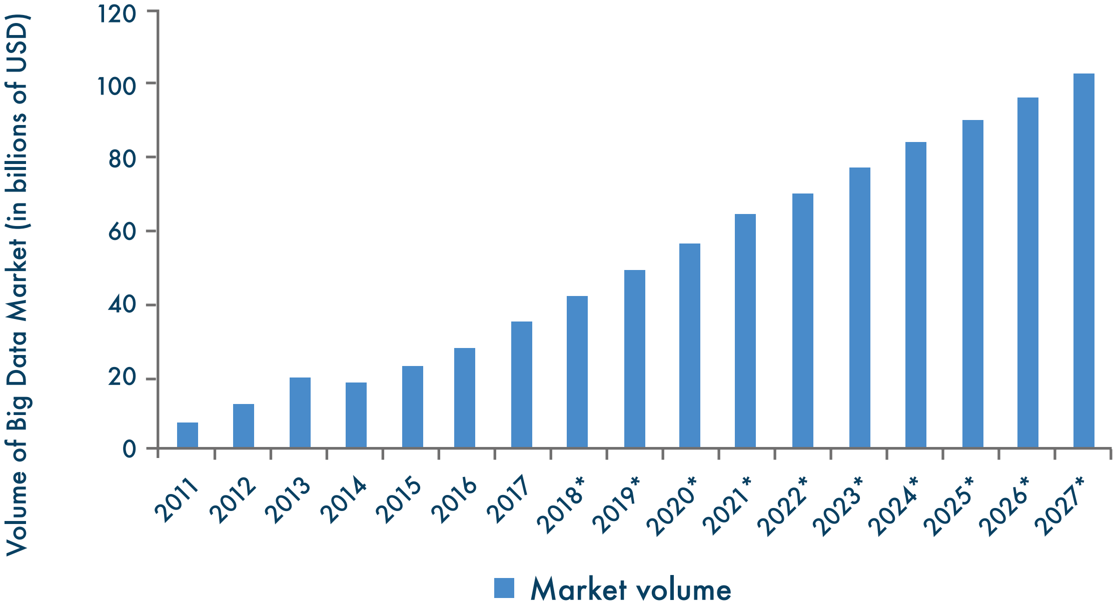
## LIST OF FIGURES

## LIST OF TABLES

## 1. INTRODUCTION

With the ubiquitous adoption of Internet and mobile technologies, data is at the core of the global digital economy. IDC estimates[1] that the number of consumers who interact with data daily, is approximately 5 billion and may rise to 6 billion by 2025, thus accounting for nearly 75 percent of the world's population. By then, according to IDC, 49 percent of the world's data will be stored in public cloud environments.[2]

Digital technology has facilitated international trade in services. Services now constitute a major proportion of global economic activity and are being delivered using electronic communication. Digital trade has lowered barriers to market entry, expanded and diversified product markets and has made the international trade climate more open.[3] Through global value chains, data generated and used in digital trade, enables the coordination of international production processes, helps small firms reach global markets and is a key input for automation in trade facilitation.[4] With products and services increasingly being tailored using data and customised to suit unique tastes and preferences, data has not only lead to operational efficiencies but has also become a determinant of competitive advantage. [5]



*Source: Statista; (*) denotes projected values*

**Figure 1.1:** Big Data Market Size Revenue Forecast (2011 – 2027)

[1] "The Digitization of the World From Edge to Core". *IDC*, 2018.

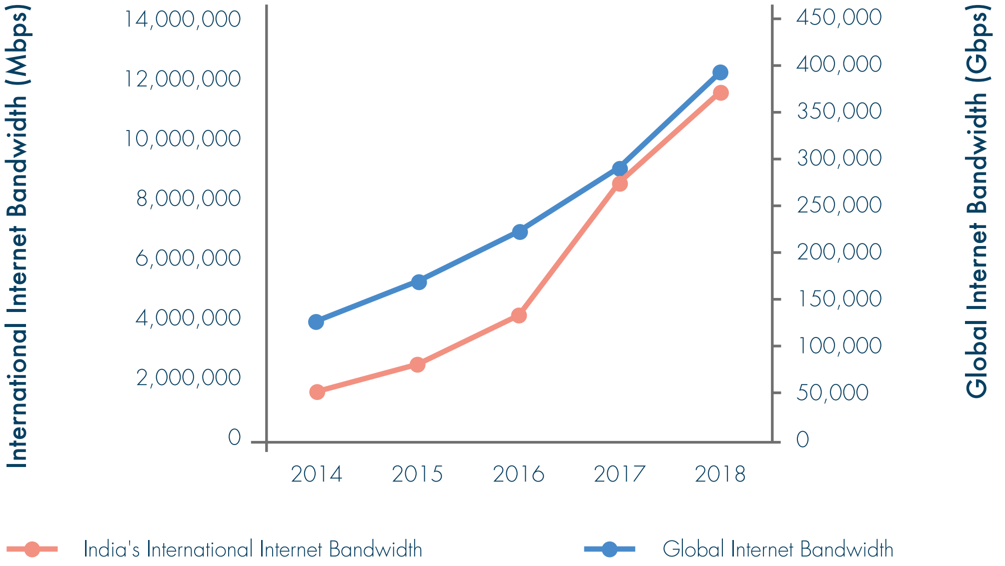
[2] *Ibid*

[3] World Trade Report – The future of world trade: how digital technologies are transforming global commerce (2018)

[4] *Ibid*

[5] "The Rise of Data Capital", MIT Technology Review Custom + Oracle

Digital transformation of global trade has made data indispensable to it. It has been argued that the constant flow of real-time information across borders is critical for emerging technologies such as cloud computing, machine-to-machine learning etc.[6] According to a 2016 report by McKinsey Global Institute (MGI), there has been a 10.1 percent increase in world GDP over the past decade, owing to all tangible and intangible flows. In 2014, this value amounted to US$ 7.8 trillion, of which, US$ 2.8 trillion i.e. approximately 36 percent was accounted for by data flows.



*Source: Compiled by authors using data from TeleGeography*

**Figure 1.2:** Increase in Internet Bandwidth (2014 – 2018)

Data has acquired the ranks of economic capital. Big data analytics are being used by businesses to reduce costs, improve decision making and generate new digital products and services.[7] Research has shown that businesses whose decision making processes are driven by data perform better in terms of output and productivity.[8] Existing literature even points to rise of the data economy as a political economic shift, wherein data is created, collected and circulated as capital.[9] This process is driven by the perpetual cycle of capital accumulation leading to capital being reliant on a world that

[6] Unleashing the benefits of free flow of data, Telenor 2018, https://www.telenor.com/wp-content/uploads/2018/04/201804_Telenor-external-FoD-position_FINAL.pdf

[7] "The Rise of Data Capital", MIT Technology Review Custom + Oracle

[8] Brynjolfsson, Erik, Lorin M. Hitt, and Heekyung Hellen Kim. "Strength in numbers: How does data-driven decisionmaking affect firm performance?." *Available at SSRN 1819486* (2011).

[9] Sadowski, Jathan. "When data is capital: Datafication, accumulation, and extraction." *Big Data & Society* 6, no. 1 (2019): 2053951718820549.

is ‘datafied’.[10] However, while businesses and society can reap benefits of big data, the potential for data, particularly personal information to be misused or be subject to malevolent practices, is also accentuated.[11]

Some countries have recently enacted regulations for data management. In some cases, these include restrictions on the cross-border flow of data, particularly personal information. In others, for example the European Union, the focus is on secure handling of personal data and not restriction on the transfer of it, per se. We show in this study that data localisation measures are not always comparable across countries, and are driven by a variety of stated policy objectives, ranging from safeguarding privacy of citizens, protecting the domestic digital economy, to safeguarding national security, among others.

## Scope of the Study

It is not only the recognisable giant internet companies like Amazon, Facebook, Google, Twitter etc. that rely on cross-border data flows to offer their services. The digital economy has also paved way for the creation and growth of micro-small and medium-sized enterprises.[12] Data flows enable access of MSMEs to new technologies like cloud computing, thus helping reduce the cost of upfront investment in digital infrastructure.[13] Data flows also facilitate their faster response to changes in demand and smoothen their process of up-scaling.[14] MSMEs gain increased access to critical knowledge alleviating information asymmetries, which help them participate in international markets, as well as compete with bigger firms.[15] MSMEs that use internet-based business models have a survival rate which is 30 percent higher than that of offline businesses and they are as likely to export as big firms.[16]

The focus of this paper is on understanding the impact of existing and proposed data localisation measures on micro-small and medium-sized enterprises in India. For the purposes of this paper, we distinguish between MSMEs and startups - the former are typically profit-making entities, while the latter depend on private equity and venture capital funding, and do not necessarily generate profits. The universe of internet-based startups in India is huge and their involvement in the digital economy distinct from that of traditional MSMEs. In the absence of sufficient data to arrive at a quantitative estimate for impacts, this paper adopts an inductive approach, extrapolating from the particular to the general. The impacts are captured by presenting use cases of MSMEs and MSME associations. The impacts have been thematically discussed. We have tried to maintain sectoral diversity in our basket of use cases.

A blanket assessment of the efficacy of a data localisation policy for India is beyond the scope of this paper. The intent has been to objectively analyse the challenges and opportunities that confront MSMEs in India due to existing and proposed measures of data localisation. The paper is organised as follows – Section 2 provides a brief overview of data localisation

[10] *Ibid*

[11] Strandburg, Katherine J. “Monitoring, datafication and consent: legal approaches to privacy in the big data context.” *Privacy, big data, and the public good: Frameworks for engagement* 1 (2014): 5-43.

[12] “Trade and cross-border data flows”, *OECD* (2018)

[13] *Ibid*

[14] *Ibid*

[15] *Ibid*

[16] Pepper, Robert, John Garrity, and Connie LaSalle. “Cross-Border Data Flows, Digital Innovation, and Economic Growth.” *The Global Information Technology Report 2016: Innovating in the Digital Economy* (2016): 39-40.

measures across the world and in India, along with the variety of rationales and motivations behind them; in Section 3 we summarise findings from our in-depth case studies and stakeholder interviews and thematically discuss impacts; Section 4 concludes the analysis and provides policy recommendations.

## 1.1 Methodology

As discussed in the section above, owing to the paucity of coherent secondary data to arrive at a quantitative estimate of the impact of data localisation on MSMEs, we conduct our analysis using qualitative methods. We present 10 use cases of MSMEs and MSME associations. The methodology adopted is the interview protocol. This approach is used to extract in-depth information about the experiences and viewpoints of participants pertaining to the topic of research.[17] For the purpose of this study, questions pertained to company profile, data storage and processing mechanisms, quantum of cross-border data flows, knowledge about data security and laws and regulations surrounding data privacy and protection, impact or potential impact of data localisation and the challenges and opportunities that such a policy might present to stakeholders, suggestions on alternatives to data localisation and allied policy preferences. While we maintained a set of fixed indicative questions, the discussions evolved based on the responses we received. Considering the sensitivity of the issue, the identities of the companies and other stakeholders interviewed, have been kept anonymous.

[17] Turner III, Daniel W. "Qualitative interview design: A practical guide for novice investigators." *The qualitative report* 15, no. 3 (2010): 754-760.

# 2. DATA LOCALISATION – AN OVERVIEW

## 2.1 Rationales for Data Localisation

The earliest regulations on data flows, most notably by the OECD,[18] can be traced back to the 1980s, before the beginning of widespread use of the internet. A recent emphasis on stricter regulation of cross border data flows was triggered in 2013 when Edward Snowden claimed that the United States National Security Agency had access to data from many internet based services, including social media.[19] This led to some countries proposing or implementing data localisation regulations, albeit in variant degrees. [20]

In the debate surrounding restrictions on cross border data flows, while one side is of the view that forced localisation is a deliberate strategy to protect domestic economy and undercut competition from big international players,[21] there is also sympathy for concerns related to data privacy, surveillance and guarding the sovereignty of countries, despite the impingement upon the free flow of data across borders.[22]

Stated rationales for localisation of data range from protection of rights of data subjects, law enforcement challenges and deflection of foreign surveillance, among others. The stated economic rationales, however, are to attract investment, fuel innovation, protect domestic industries and create competitive advantage for domestic companies.

Arguments in favour of data localisation often emphasise security concerns. Some countries have stated that, in the absence of binding international rules on cross-border data flows, data localisation is the most feasible measure by which they can ensure the privacy and protection of their citizens.[23] Indian government agencies have argued that it would be easier for law enforcement agencies (LEAs) to mitigate criminal activities if the relevant data were to be stored in India. State functionaries have also argued that existing data sharing arrangements can make the process for LEAs much more prolonged and legally complex. Moreover, the Srikrishna Committee Report argues that data localisation can be beneficial to the Indian economy by incentivising the development of digital infrastructure for data storage and processing. Specifically, it highlights the increased opportunities for India's economy through the use of data analytics based on artificial intelligence. Proponents of data localisation in India have also argued that moving data storage to India would generate more jobs.

Arguments against data localisation have highlighted its costs and questioned its benefits. Data localisation has been considered a trade barrier in the digital age. Such policies are likely to hamper trade in services, particularly those that use telecommunications and internet infrastructure. Cutting off data flows, erecting barriers to them or making them more

[18] Kuner, Christopher. "Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future. *OECD Digital Economy Papers, 187,* (2011)

[19] *Op Cit*, 16

[20] Ferracane, Martina. "Restrictions on Cross-Border data flows: a taxonomy." (2017).

[21] Chander and Le (2014); Aaronson and Maxim (2013)

[22] Rubin (2015); Kong (2010); Gurumurthy et al. (2017)

[23] Panday (2017)

expensive not only puts foreign firms at a disadvantage,[24] but by protection of local firms from foreign competition, it aggravates the challenges to their potential participation in global markets.[25] Data localisation could also pave way for state surveillance of own citizens. This will have serious implications for personal privacy and citizens' rights.

Implementation of data localization poses several challenges. While foreign entities such as Amazon, Google, Microsoft and domestic companies like RCom, CtrlS, Sify have data centres in India, expanding this infrastructure may be difficult. Data centres require, *inter alia*, dependable power supply, which could be a challenge in India. Several businesses have expressed their concerns over additional, recurring costs of data storage and management in India, in the event of a data localisation mandate. Duplicating overseas data in order to mirror and then localise it would incur its own costs, and it would also ignore cheaper foreign alternatives for data storage.

Data localisation, it is argued,[26] is the antithesis of the fundamental architecture of the internet and could lead to its "balkanisation". Such measures might entail routing of data through more long-winded and less efficient networks. Local data storage will necessitate that data be transferred from global to local servers, leading to increased investments in data management infrastructure and therefore, additional costs for businesses. Data localisation would likely make data more vulnerable to security breaches, by preventing "sharding" as all information would be stored in one place. Sharding is a process that ensures different rows of databases are in different servers across the world, and thus "shards" provide enough data to operate but they mask the identity of data subjects. It has also been argued that localisation is likely to hinder innovation.

Several studies have estimated the economic costs of data localisation. For instance, a study conducted by the Leviathan Security Group in 2015 found that local companies would be required to pay 30 – 60 percent more for their computing needs in the event of forced data localisation legislation. Another study conducted by Bauer et al. in 2016 found that data localisation and commonly used barriers to data flows decreased Total Factor Productivity (TFP), which further reduced GDP by 0.1 percent in Brazil, 0.55 percent in China, 0.48 percent in the EU and 0.58 percent in South Korea. In some cases, data localisation also necessitates the construction of data centres in the concerned countries, which can add to the costs incurred by business enterprises. A study conducted by Trevisiani and Chao in 2013 estimated the average cost of setting up data centres in selected countries and found that the cost for Brazil was US$ 60.9 million, for Chile, US$ 51.2 million and for the U.S., US$ 43 million, with operating costs (energy and other expenses) at a monthly average of US$ 950,000 in Brazil, US$ 710000 in Chile, and US$ 510,000 in the US.

## 2.2. Data Localisation Measures across the World

Several countries – though, a small minority overall – have adopted, or are in the process of adopting data localisation measures. Their rationale, nature, degrees of stringency and legal provisions are vastly different, however. These measures vary depending on the country and its unique legislative traditions. For example, the European Union emphasises, privacy as a human right and seeks to create legally binding instruments whereas the measures proposed for the APEC region focus more on the advantages of e-commerce. Another example of data localisation is Australia's My Health

[24] USITC (2016)

[25] IAMAI (2016); UNCTAD (2016)

[26] Fraser, Erica. "Data Localisation and the Balkanisation of the Internet." *SCRIPTed* 13 (2016): 359.

Records Act of 2012, which requires all personally electronic health records to be stored in local data centres. Therefore, no electronic health records can be held or processed outside Australia, unless they are *not* personally identifiable or *not* in relation to a consumer.[27] An amendment to this was passed in 2018, under which the operator of My Healthcare Records system in Australia could not disclose data to law enforcement or government agencies without a judicial order or the healthcare recipient's consent.[28] Moreover, for those who have cancelled their My Health Record, all data pertaining to them needs to be permanently deleted from the National repositories service.[29] Similarly, Russia's data localisation law prohibits personal data transfer of Russian citizens across borders and requires that it be stored within Russian servers.[30] Germany has also implemented[31] data localisation by requiring the processing and storage of public sector data on "Bundescloud". The examples above only provide a snapshot of the various explicit and implicit requirements of data localisation implemented by several countries.

Enacted in May 2018, the European Union's General Data Protection Regulation (GDPR) is possibly the most comprehensive data protection policy of recent times. However, it does not mandate data localisation per se. Instead, it prescribes standardised data protection laws across the EU. The GDPR offers greater protection and rights to citizens including easier access and control of their data.[32] It covers both personal and sensitive data.[33] Compliance with GDPR requires companies to define their data protection policies, conduct audits and impact assessments of data protection and document their data processing mechanisms.[34] Notably, in November 2018, the EU also introduced a legislation that prohibited member states from data localisation requirements for non-personal data unless they meet the proportionality criteria solely on ground of public security. [35]

Recently, the United States enacted the Clarifying Lawful Overseas Use of Data (CLOUD) Act. This enables executive authorities to legally request for data stored abroad by entities bound to US jurisdiction and have over their data.[36] The CLOUD Act has been subject to criticism. For example, Germany claims that its data on Amazon's cloud could be available to US agencies and would also violate Germany's data protection legislation.[37] On the other hand, it has been argued that the act would enable foreign governments to enter into a bilateral executive agreement[38] with US to obtain access to data in possession, control, or custody of US entities.

[27] https://www.aph.gov.au/Parliamentary_Business/Bills_LEGislation/Bills_Search_Results/Result?bId=r 6169

[28] *Ibid*

[29] *Ibid*

[30] *Ibid*

[31] https://www.insideprivacy.com/cloud-computing/germanys-criteria-for-federal-use-of-cloud-services/

[32] https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018

[33] *Ibid*

[34] *Ibid*

[35] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union

[36] "Demystifying the U.S. CLOUD Act: Assessing the law's compatibility with international norms and the GDPR". *Hogan Lovells* (2019).

[37] https://www.politico.eu/article/german-privacy-watchdog-says-amazon-cloud-vulnerable-to-us-snooping/

[38] *Op Cit,* 30

Regulation of cross-border data flows has been prevalent in China since 2011. China is said to have the most restrictive data protection laws in the world. Articles 24 and 61 of its legislation require all telecommunication and instant messaging service providers to register the real name of its users and provide that data to the government for law enforcement[39] purposes. The beginning of China's policy can be traced to the time when China's Central Bank directed that financial information gathered in China's regional territory must be stored, processed, and analysed only within China's jurisdiction.[40] Further, according to its new draft policy, all companies - domestic and foreign - must store their data in Chinese data centres only.[41] China has been characterized as a high risk zone for data centres by ranking 35 out of 37 countries in Cushman and Wakefield's 2016 Data Centre Risk Index. However, the Draft Measures on Security Assessment of Cross-Border Transfer of Personal Information, in China, was recently released for public comments and it doesn't propose express localisation requirements. Although it provides for thorough security assessments to be conducted for cross-border transfer of data.[42]

## 2.3 Data Localisation Measures in India

Data localisation measures and legislation in India date back to 1993 with the Public Records Act and the Unified Access License for Telecom Services in 2004. The measures under these legislations were implicit and were undertaken for the protection of sensitive data much before the extensive proliferation of the internet and data we see today. The Public Records Act prohibits the transfer of public data outside the Indian region, barring exceptions. This Act requires that transfers of public records are only made with prior permission from the central government or for official purposes only.[43] Furthermore, in 2014, the Government of India executed the MeghRaj initiative, which has localisation requirements for public records and data owned by the Government of India.[44] This is reportedly, imposed through regulatory structures and procurement contracts.[45] The stated objective behind this initiative was to promote cloud computing, make e-service delivery systems more efficient, and augment the government's ICT expenditure[46] by promoting the setting up of data centres, and associated physical and virtual hardware within India.[47]

Data localisation is also required by many sectoral regulations. Holders of the Unified Access License, which includes, inter alia, all telecommunications and internet service providers, are prohibited from transporting user information and any other information related to subscribers, aside from international billing uses, outside of India.[48] Under the IT Act of

[39] https://jsis.washington.edu/news/chinese-data-localization-law-comprehensive-ambiguous/

[40] *Ibid*

[41] *Ibid*

[42] https://www.huntonprivacyblog.com/2019/06/19/china-issues-draft-regulation-on-cross-border-transfer-of-personal-information/

[43] See Section 4 of the Public Records Act 1993

[44] http://www.nishithdesai.com/fileadmin/user_upload/pdfs/NDA%20In%20The%20Media/Quotes/ 180405_Q_indrastra.com-MeghRaj__Indias_Cloud_Initiative.pdf

[45] *Ibid*

[46] https://cloud.gov.in/about.php

[47] Bailey and Parsheera (2018)

[48] *Ibid*

2000, sensitive personal data is permissible to be transferred by a corporate entity to another entity or person within or outside of India only if  the other person or entity reciprocates the same level of data protection.[49] The Act is not considered to be a dedicated law on data protection, privacy and security. Notably, the Act does not deal with third party data transfers, cross-border movement of personal data, the data sharing ecosystem, along with knowledge and consent of data subjects about what use their personal data is being put to.[50] The constitution of the expert committee on data protection, headed by former Supreme Court Chief Justice B.N Srikrishna, and subsequently the white paper released in 2017 and the draft Personal Data Protection Bill released in 2018 prompted the recent debate on data localisation in India.

The Bill categorises data into personal and sensitive personal data, which are defined as follows:

*Personal Data: Data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic trait, attribute, or any other feature of the identity of such natural person, or any combination of such features, or any combination of such features with any other information.*

*Sensitive Personal Data: Personal data revealing, related to, or constituting, as may be applicable – passwords; financial data; health data; official identifier; sex life; sexual orientation; biometric data; genetic data; transgender status; intersex status; caste or tribe; religious or political belief or affiliation or any other category of data specified by the Authority under section 22.*

The Bill stipulates that one copy of any personal data of Indian citizens must be stored in servers located in India. While the government may exempt certain categories of data from this provision for reasons such as necessity or state security, it may not do so for sensitive personal data. The report also includes a third category entitled critical personal data - not defined in the bill- which must only be stored on servers in India.

Over the years, many proposals regulating data flows have been proposed or implemented across a multitude of sectors. In April 2018, Reserve Bank of India (RBI) ordered  localisation of all data by providers of payment services.[51] In addition, In May 2018, India's health ministry formulated legislation to protect the health data of citizens by giving citizens complete ownership of their personal health data. Furthermore, In July 2018, telecom regulator TRAI stated[52] that all organizations which handle or manage consumer data need to be regulated. More recently, there was a proposal on e-commerce policy for data localisation. In February 2019, the draft was revised to contain localisation requirements and included restrictions on cross-border transfer of data generated by IoT[53] devices located in public places, e-commerce platforms, social media, etc. It also legally binds organisations that store their data overseas to not share their data with a third party. Figure 2.3 provides a timeline of some key instruments of data regulation in India.

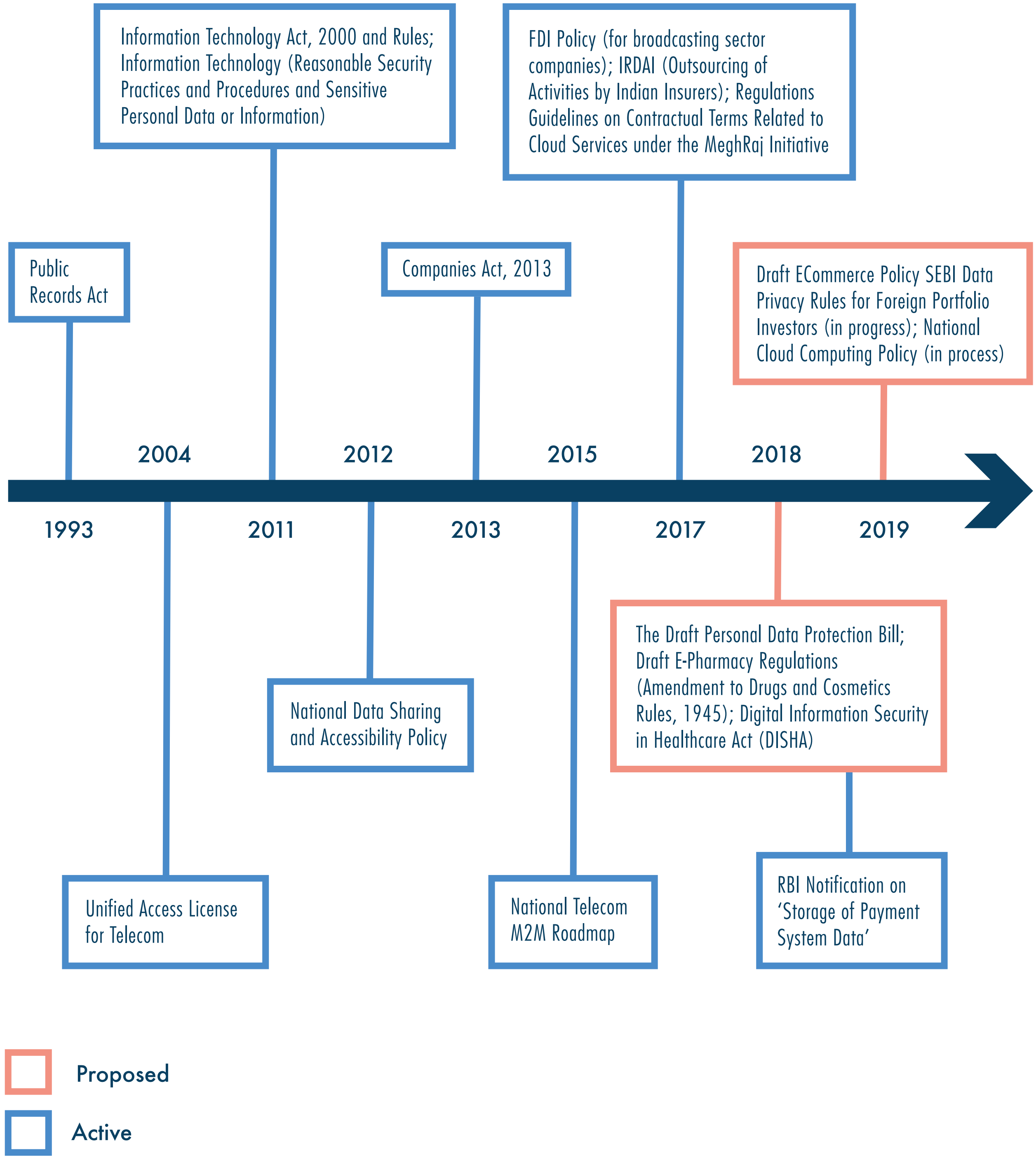
[49] https://www.ikigailaw.com/data-localisation-requirements-for-telecom-and-internet-service-providers-current-law/#acceptLicense

[50] Clarification on Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules 2011 under section 43A of the Information Technology Act, 2000. https://www.meity.gov.in/writereaddata/files/PressNote_25811.pdf

[51] https://rbidocs.rbi.org.in/rdocs/notification/PDFs/153PAYMENTEC233862ECC4424893C558DB75B3 E2BC.PDF

[52] https://main.trai.gov.in/sites/default/files/RecommendationDataPrivacy16072018_0.pdf

[53] Internet-of-things


Public Records Act
1993
Information Technology Act, 2000 and Rules; Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information)
2004
Unified Access License for Telecom
2011
Companies Act, 2013
2012
National Data Sharing and Accessibility Policy
2013
FDI Policy (for broadcasting sector companies); IRDAI (Outsourcing of Activities by Indian Insurers); Regulations Guidelines on Contractual Terms Related to Cloud Services under the MeghRaj Initiative
2015
National Telecom M2M Roadmap
2017
Draft ECommerce Policy SEBI Data Privacy Rules for Foreign Portfolio Investors (in progress); National Cloud Computing Policy (in process)
2018
The Draft Personal Data Protection Bill; Draft E-Pharmacy Regulations (Amendment to Drugs and Cosmetics Rules, 1945); Digital Information Security in Healthcare Act (DISHA)
RBI Notification on 'Storage of Payment System Data'
2019
Proposed
Active

*Source: ICRIER (forthcoming, 2019)*

**Figure 2.1:** Timeline of Key Instruments of Data Regulation or Localisation in India

Data localisation has both proponents and opponents. Some of the government's stated objectives include enabling innovation, improving cyber security and privacy, enhancing national security and protecting against foreign surveillance.[54] As per the draft Data Protection Bill, 2018, development of an indigenous ecosystem of artificial intelligence can be a key driver of economic growth and such innovation can be aided by storing data in India and granting Indian start-ups access to anonymised versions of the data.[55]

Data localisation has also attracted significant criticism. After RBI's directive for local storage of payments data, global card companies such as  MasterCard raised concerns that the directive would  adversely affect the fraud detection system and the detection of money laundering in  domestic payments.[56] The directive requires payment companies to store data of Indian users exclusively on local servers and the deletion of back data from global servers as well, which according to public comments from MasterCard, is a requirement unique to India.[57]

India's draft e-commerce policy has also drawn criticism.  It was highlighted by the 2019 National Trade Estimate Report on Foreign Trade Barriers by the US Trade Representative, that India's data localisation requirements would act as significant barrier to digital trade between India and the US.[58] According to the report, localisation requirements would raise costs for suppliers of data-intensive services as they would be forced to construct additional data centres in India.[59] Data localisation would also prevent domestic firms from taking advantage of available global services that might be more feasible both in terms of costs and quality.[60] Opponents view protection of domestic firms as the overriding objective of localisation. Besides, government would get 'unfettered' access to domestic user data and help foster innovation through easier access to locally stored data for home-grown start-ups. The benefit to domestic companies has to consider the possibility that  small and medium sized foreign start-ups may not want to scale to India on account of additional compliance costs for data localisation.[61]

[54] "The Localisation Gambit". *The Centre for Internet and Society* (2019)

[55] *Ibid*

[56] https://www.livemint.com/companies/news/rbi-data-localisation-rule-may-compromise-fraud-detection-in-india-mastercard-1552889014479.html

[57] https://www.livemint.com/Companies/MzB7AcmM9mOarQKh0BIn5J/Mastercard-will-delete-Indian-cardholders-data-from-servers.html

[58] https://www.livemint.com/industry/retail/us-criticises-india-s-data-localisation-norms-draft-e-commerce-policy-1554806134762.html

[59] *Ibid*

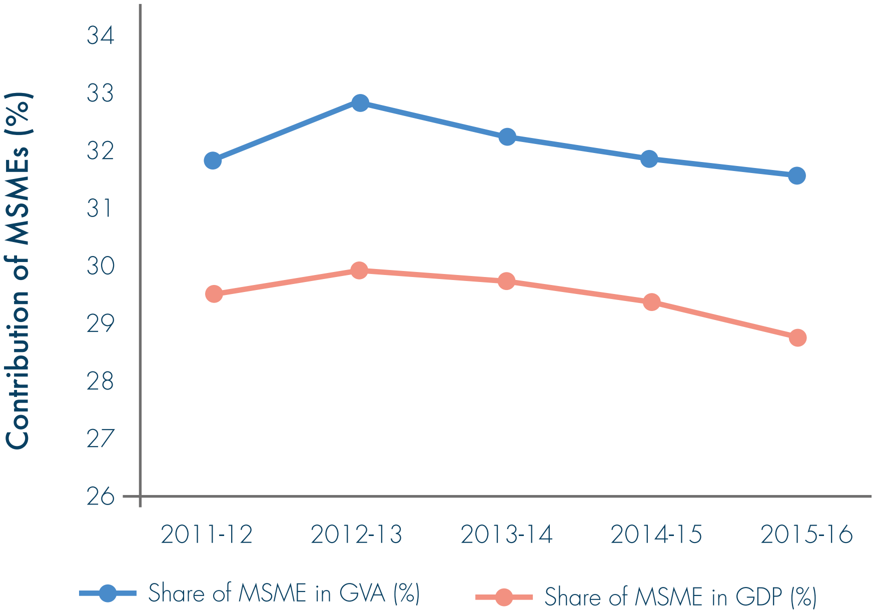
[60] *Ibid*

[61] https://qz.com/india/1422014/rbis-data-localisation-could-hurt-indias-own-startups/

## 3. IMPACT OF DATA LOCALISATION ON MSMES

### Insights from Case Studies and Stakeholder Interactions

Micro-small and medium enterprises (MSMEs) have been drivers of growth in the Indian economy. There are approximately 64 million MSMEs in India.[62] The sector is the second largest creator of jobs in the country.[63] According to the 73rd round of the NSS, the contribution of MSMEs to employment in terms of number of employees is over 110 million.[64] In the period 2011-2016, micro-small and medium enterprises (MSMEs) contributed roughly 29 percent of India's GDP and over 30 percent of Gross Value added (GVA).[65] They are India's most important source of employment. In 2015-16 over 120 million found employment in MSMEs across India's diverse economic terrain. Many of these enterprises have demonstrated great initiative and innovation in use of digital services. The classification of such enterprises according to the MSME Development Act, 2006, is given in Appendix 1.



*Source: Compiled by authors from the Annual Report (2017-18) of the Ministry of Micro, Small and Medium Enterprises*

**Figure 3.1:** MSMEs' Contribution to GVA and GDP (2011 – 12 to 2015 – 16)

[62] 73rd Round of the NSS

[63] https://yourstory.com/smbstory/how-msmes-are-helping-india-become-a-financially-i-hdxm3ljlqh/

[64] https://msme.gov.in/sites/default/files/MSME-AR-2017-18-Eng.pdf

[65] https://msme.gov.in/sites/default/files/MSME-AR-2017-18-Eng.pdf

Adoption of technology among MSMEs in India has not been uniform. A survey conducted by Yes Bank in January 2019 found that out of 2700 surveyed MSMEs, only 5 percent had adopted digital technology, where full scale technology adoption included the use of cloud services, account management software, digital banking etc.[66] The survey found that major hindrances to technology adoption among MSMEs in India, included lack of knowledge to choose the right technology solutions or of their impact on profitability, lack of skilled labour to operate technology, lack of trust in technology based solutions and high costs of equipment.[67] However, high levels of technology adoption were found in MSMEs in sectors like IT, ITeS, food processing, engineering, manufacturing, healthcare and pharmaceuticals.[68] MSMEs in education have also adopted technology. For example, an MSME, Safeducate, uses AI operated vans which act as virtual reality-led experiential centres for students and gives them glimpses of jobs in retail, manufacturing, warehousing etc.[69]

India also has a vibrant startup economy. According to a recent report by KPMG, the number of startups in India has increased from 7000 in 2008 to 50,000 in 2019 and one of the factors driving this explosion has been the rise of digital technology and opportunities in the digital economy.[70] According to a study by NetApp and Zinnov, B2B startups increased from 900 to 3200 between 2014 and 2018.[71] More than 75 percent of India's B2B startups work in the areas of artificial intelligence, internet-of-things and robotic process automation, and these new technologies in turn have  contributed to the rise of these startups.[72] Startups operate in a vast array of industries, ranging from financial services to hospitality, from e-commerce to  education, logistics and many more. Several startups have attained unicorn status and enjoy valuations in upwards of billions of dollars. Examples include Paytm, OYO, Byju's, Swiggy etc. Popular startups such as Ola and Zomato have also scaled up to countries outside of India. Figure 3.2 gives a sector-wise distribution of tech-startups in India.

[66] https://www.financialexpress.com/industry/sme/only-5-msmes-have-fully-embraced-digital-technology-says-yes-bank-survey/1447985/

[67] *Ibid*

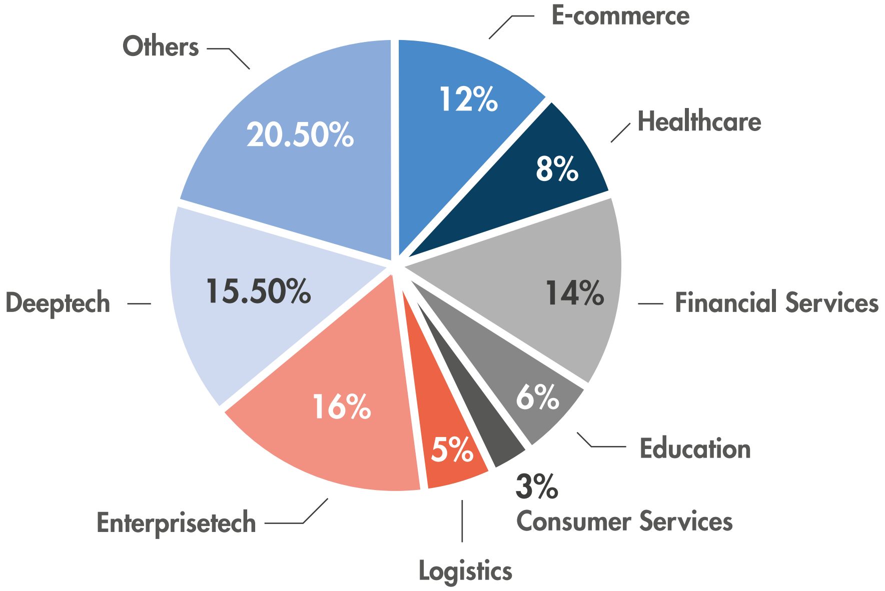
[68] *Ibid*

[69] https://yourstory.com/smbstory/indian-msmes-too-are-adopting-technological-innova

[70] https://entrackr.com/2019/02/startups-india-grew-50k-2019/

[71] https://yourstory.com/2019/05/b2b-tech-startups-india-netapp-zinnov

[72] *Ibid*



*Source: Compiled by authors from "Maharashtra and the exciting growth of its startup ecosystem", KPMG, February 2019*

**Figure 3.2:** Sector-wise Distribution of Tech-Startups in India

### 3.1 Framework for Selection of Case Studies

The analysis in this section is based on 10 in-depth interviews with MSMEs as well as MSME associations. Our sample consists of 8 enterprises and 2 MSME associations. The focus, however, has been on those with internet-based delivery models. We have attempted to cover a diverse set of sectors. The number of employees in the companies has been used to classify them as into micro, small or medium enterprises. As per OECD's classification, micro enterprises have less than 10 employees, small enterprises have 10 to 49 employees, medium-sized enterprises have 50 to 249 employees and large enterprises employ 250 or more people.[73] To respect the confidentiality of the inputs provided by stakeholders, the analysis has been anonymised. 7 out of the 8 enterprises are of Indian origin with their offices located in India. 1 enterprise is of foreign origin with its headquarters located in the UK and an operational office in India. Through the case study analysis, we have attempted to provide a nuanced understanding of the use of data in small businesses, their data management processes, quantum of cross-border data flows, and their awareness of policies on data security. We also attempt to capture the compliance costs and regulatory burden due to data localisation policies. It is clear even from our early analysis that the ability of MSMEs to adapt to data localisation is evidently heterogeneous. Table 3.1 provides an overview of the stakeholders interviewed.

[73] https://data.oecd.org/entrepreneur/enterprises-by-business-size.htm

**Table 3.1:** Case Study Framework

| Sector of Operation | Type of Organisation | Year of Incorporation | No. Of Employees | Classification of Enterprise | Company Origin/ Headquarters | Country/ Countries of Operation |
|---|---|---|---|---|---|---|
| *Financial Services* | Private | 2015 | 51 – 200 | Medium-sized enterprise | India | India |
| *Education and Digital Marketing* | Partnership | 2005 | 51 - 200 | Medium-sized enterprise | India | Located in India, but has clients primarily in the United States. Their business model allows them to have clients across the world. |
| *IT Software and Services (SaaS)* | Private | 2008 | 51 - 200 | Medium-sized enterprise | India | Located in India, but has clients across the world, primarily in the United States. Their business model allows them to have clients across the world. |
| *Education and Networking* | Private | 2015 | 11 - 50 | Small enterprise | India | India. Their users are spread across the world. |
| *Agriculture and Financial Services* | Private | 2015 | 1 - 10 | Micro enterprise | India | India |
| *Research and Development* | Private | 2012 | 7 plus contractual labour | Micro enterprise | India | India |
| *Digital Marketing and Software Products* | Private | 2015 | 2 - 10 | Micro enterprise | India | Office located in India. Clients located in India and overseas. |
| *Management Consulting and Marketing Services* | Private | 2014 | 2 - 10 | Micro enterprise | United Kingdom | India and UK. Clients across the world. |
| *MSME Association 1* | Not applicable | No information available | Not applicable | Not applicable | India | India |
| *MSME Association 2* | Not applicable | 2005 | Not applicable | Not applicable | India | India |

*Source: Compiled by authors based on stakeholder interviews*

## 3.2 Findings from Case Studies

MSMEs rely on digital technologies to varying extents. Not all of them store or process personal data. Dependence of their business on data transfer across national borders varies widely. In most cases, the impact of data localisation would depend on multiple factors. These include, inter alia, the nature of the MSME's business, its location, demography of its customers, as well as of its competitors etc. It is therefore possible that a large Indian e-commerce service targeting overseas customers may escape the immediate impact of data localisation. On the other hand, a taxi service, with a predominantly local customer base could face new compliance challenges, if the data is currently stored overseas and if data localisation measures were to be enforced. Any analysis of impact of data localisation on MSMEs is therefore best seen as indicative.

The findings from our analysis have been discussed under three themes – *data storage and management processes of SMEs* (highlighting sector wise variations), *impact of data localisation on MSMEs*, and *opinions and preferences for policy*, as indicated by MSMEs. Appendix 2 provides company wise details.

### 3.2.1 Data Storage and Management Practices

MSMEs typically have limited resources and are unable to invest too much in building in-house IT infrastructure. All enterprises in our sample reported storing personal data, albeit in varying quantities and with varying degrees of sensitivity. Instead of running their own data centres, all enterprises reported using third party cloud service providers. There was a wide preference for international cloud service providers like AWS, Google and Azure, over Indian cloud service providers. The primary reason cited by MSMEs is the high quality of associated services, such as, for example, sophisticated AI analytics offered by AWS in its overseas data centres. There is also a general perception that data security arrangements of international cloud service providers such as AWS, Google and Microsoft, are stronger relative to their Indian counterparts. Enterprises highlighted that using international cloud storage was more flexible and cost effective.

Except for an enterprise in the edutech sector, all enterprises highlighted enhanced security on third party clouds. The edutech company reported that after scaling up significantly, it would invest in its own data centre located in India, preferably in the vicinity of its physical location, for ease of access. Currently, it reported storing its data on a third-party cloud located in India. According to it, security would be enhanced in its own data centre. Despite the operating expenses, in-house data storage infrastructure would be an asset if it went in for public listing in the future. Most of the enterprises in our sample reported that a large proportion of their clients belonged to countries like the US. This was one of the primary reasons cited for storing their data in countries outside of India.

The most popular choice of location for data storage by MSMEs seemed to be the US, followed closely by Singapore. The basket of services available overseas was more diverse and the cost of data storage and processing much lower. It was highlighted that international cloud service providers introduced new features and services first in these data centres, before they were introduced in India, (presumably because Indian data centres of international service providers are relatively new and have been operational only in the last few years). However, this makes data storage outside India an important competitive advantage.

A financial services startup of Indian origin, which operates exclusively in India, reported that following the RBI's directive to store payments data in India, it had to migrate their data stored on cloud in Singapore. This was the only enterprise in our sample that reported segregating sensitive data of users from the overall data collected. They reported that this data is stored separately and encrypted, following industry encryption standards.

A crucial problem, however, is that not all MSMEs segregate personal and sensitive personal data from the overall data they collect. MSMEs with overseas customers did not report segregating data by geography. Moreover, there was a serious lack of awareness about policies related to data. An edutech-cum-digital marketing MSME acknowledged limited understanding of data usage, storage and security and being unaware of steps to strengthen security and address data breaches. An MSME organization highlighted that this lack of education and awareness puts MSMEs at the risk of inadvertently violating the law and therefore, bearing its consequences.

All the MSMEs in our sample routed their payments through a third-party payments gateway and therefore did not store any financial data. A logistics company that has recently diversified into fintech and works with NBFCs to extend credit to farmers reported storing financial data. However, it is not yet compliant with RBI's guidelines for local storage of payments data. It also exhibited a preference for foreign cloud service providers over their Indian counterparts citing the lack of full stack of options with the latter. They observed that foreign cloud services offered better compatibility between front and end user applications. This was an important consideration for businesses like theirs that are driven by technology.

A management consulting and marketing enterprise of foreign origin operating in India, reported storing data on platforms like Dropbox and Boxcrypter, that have their data centres located outside of India. The company highlighted that none of its clients have requested for their data to be stored in India, thus far. It noted that while it is possible to move their data storage infrastructure to India, it would involve additional costs and inconvenience. Furthermore, according to it, there was overall reluctance among the business community in the EU to store data in India due mainly to concerns about India's data security infrastructure and power shortages. This can act as a crucial impediment to building and maintaining data centres in India.  Thus, for most MSMEs interviewed for this study, India did not seem to be a natural choice for data storage and management. Most of them reported a preference for storing data outside India because of a high proportion of overseas customers. Except for the edutech company in our sample, none of the other enterprises had their data localised. Moreover, there was a clear preference for international cloud service providers as compared to Indian cloud service providers, as the latter's services were perceived to be expensive and often short of global standards. Some even expressed concerns about the level of data security in Indian data centres. The edutech-cum-digital marketing enterprise expressed concerns over the nearly non-existent data security framework. Some stakeholders felt foreign governments to be more supportive of high quality data storage infrastructure in their countries.

### 3.2.2 Impact of Data Localisation

The impact of data localisation appears to vary between sectors. While some enterprises reported a significant cost burden, some others have reported no potential impact. A software products and services company reported storing limited amount of personal data about their customers. Moreover, only 5 percent of their customers are from India. Therefore, for complying with data localisation, they would have to segregate Indian citizens' data from the rest of the data. Considering the small consumer base, such segregation would incur high costs and compliance to data localisation would be challenging. It would lead to an increase in their development and maintenance costs. At the application level, the cost incurred was estimated to be Rs. 200,000 - 250,000, while changes in data storage infrastructure could entail an additional Rs. 15,000 per month. It would also be difficult for the enterprise to maintain multiple data storage infrastructure. Overall, data localisation could entail 10 percent to 15 percent additional costs including management overheads.

Similarly, a digital marketing and software products company highlighted that only 5 percent to 10 percent of all its data belongs to Indian citizens. Therefore, segregating this data would be challenging. In the event of a data localisation mandate, the enterprise would have to buy server space and establish a separate team to handle data management. The additional cost of compliance for the enterprise was estimated to be at least, Rs. 100,000 per month. For a micro enterprise this could be a significant burden. They also highlighted that with the already higher costs due to goods and services tax (GST), additional costs from data localisation could render the business unviable. Furthermore, cost increases and compliance with data localisation might be easier for big companies owing to their economies of scale and bargaining power. In the event of data localisation, the company could be compelled to shift to a possibly cheaper but poorer quality service even though those provided by the bigger and global market players were superior to their Indian counterparts. Their costs could rise by typically 40 percent if they were to move to an Indian cloud service provider offering services of comparable quality.

For an edutech-cum-digital marketing enterprise, with all its clients based outside of India, data localisation laws in India may not apply directly. However, the impact could be indirect. The enterprise reported storing personal data, such as, database of students and their details, in case of foreign universities which are its clients. Therefore, if it were to store personal data of students enrolled in a foreign university, which is its client, then the database might include personal data of the university's Indian students which might be subject to localisation requirements. The enterprise also cited examples of some Indian citizens who run businesses in Dubai and use their digital marketing services. In such cases, it is impossible for the company to segregate the data. Data segregation and compliance costs incurred would be at least US$ 15,000. This estimate was based on the cost incurred by the enterprise to carry out third party data security audits sought by one of their clients. The value highlights the cost of restructuring servers and carrying out a vulnerability assessment. However, they mentioned that this would be a one-time cost.

Despite being part of several industry bodies, MSMEs highlight an acute lack of knowledge of GDPR or data protection in general. There are few consultants to guide them on implications of data breaches. The cost estimate provided by them would probably be incurred if they hire a third-party agency to segregate the data, set up more servers and do a vulnerability assessment to assure data security. Currently the company pays Rs. 25,000 to a global cloud service provider and expects this cost to double if it has to comply with data localisation rules. Furthermore, as a company operating in India, its biggest competitive advantage comes from its lower operating costs. This would be lost if some of the additional compliance costs had to be transferred to their customers. Therefore, the costs of data localisation would make their business less competitive and hurt profits.

As discussed in the previous subsection, MSMEs in our sample reported using third party payment gateways. RBI's guidelines in April 2018 mandating local storage of payments data affected several companies in the sector, both big and small. Two of the enterprises in our sample – the aforementioned edutech-cum-digital marketing enterprise and a software products and services enterprise – reported using the services of a global payment gateway for transactions on their website. If these payments companies incur significant compliance costs, it is likely that they would have to transfer some of the costs to their customers. If the cost burden is exceptionally high, they may need to shut operations. Both enterprises highlighted the importance of using a payment gateway set up by globally trusted brands. The edutech-cum-digital marketing enterprise highlighted that their business could close down without such a global payments gateway. In the absence of an internationally reputed brand, their customers would be concerned about the security of their transactions. Prominent global payments companies, it was reported, have buyer and seller protection programs to build trust in the security of transactions. The enterprise currently pays approximately 7 percent of its earnings to avail the services of the payment gateway. It would hurt their profit margin, if compliance costs incurred by the payments company were to trickle down to the enterprise.

The aforementioned software products and services company, as well as a digital marketing enterprise reported that they would consider setting up a subsidiary in another country to process payments there if compliance costs of their chosen payments gateway were to trickle down to them, The software services enterprise observed that they would switch to using services of a company like Strike that offers a feature called Strike Atlas that would help them launch a legal entity/ subsidiary in the US  which would not be subject to RBI guidelines. This alternative, it was mentioned would be more cost effective. Currently, the company pays 10 percent of its total revenue to the payment gateway. This includes costs of currency exchange which would be considerably lower with such a US subsidiary. This would also be a superior option for the company's US clients. However, this would hurt India's export revenue.

A management consulting and marketing company, headquartered in the UK and operating in India highlighted that data localisation rules would compel them to operate two data centres – one in India and another overseas. This is because its work in both locations is heavily integrated. While it would be possible for the company to shift its entire data storage infrastructure to India, there would be uncertainty surrounding the level of security and the quality of storage services would have to match up to those they avail of overseas. They would require regular audits of internal systems of third party providers of data storage services to ensure quality and data security. There would be upfront costs involved in checking their compliance with Indian data localisation requirements. Data localisation could therefore add a layer of complexity to the operations of foreign firms in India, and dent the ease of doing business. According to the company, rates of data storage on cloud are designed with big businesses in mind.

The same MSME highlighted another complexity stemming from data localisation. This related to increasing use of SaaS ("Software as a Service") applications such as, for example, the Zoho suite targeted to MSMEs. The MSME would have little say or control on choice of data centres by providers of SaaS services. It mentioned also that apart from financial costs of compliance with data localisation, teams in additional locations would need to be trained to understand the regulations and the conditions for compliance. This would add to the costs already incurred in complying with the GDPR.

Some enterprises, however, reported that there would be no impact of data localisation on them. For an edutech company, that already has its data localised, argues that localisation of data is important and would be beneficial to Indian MSMEs and startups. A logistics-cum-fintech enterprise reported that although they currently store their data on cloud in the US, the quantum of that data is not very large. so their migration costs would be low. Another logistics enterprise that has pre-emptively localised its data reported that the reason behind such a step was to avoid a surprise implementation of data localisation rules since a shorter time window to comply could raise costs. A research organisation we interviewed, did not report storing any personal data apart from that of their own employees. However, it reported storing this data in its own servers, and therefore already localised. An MSME association was of the belief that data localisation is an anti-free trade and anti-innovation measure, as innovation can foster only in a free market environment. None of the enterprises, except for the edutech enterprise believed that location of data storage determined its security. Enterprises were also of the view that forcing data localisation on MSMEs could put some out of business in India, thus jeopardising a critical driver of the economy and hurt revenue to the state.

### 3.2.3 MSME perspective on Policies for data protection and security

The predominant concern of MSMEs and associated stakeholders was their acute lack of awareness of policies surrounding data privacy. The resounding suggestion for policy was twofold – first, to educate MSMEs on the benefits of leveraging the digital economy and data to grow their businesses and second, to disseminate information on laws governing the data economy and firms' regulatory obligations. An MSME association observed that currently, MSMEs are not even aware of the amount of data used or created by them and are therefore its regulatory implications. For instance, for enterprises in the logistics and shipping sector, pushing out shipments generates a lot of data. MSME's are often unmindful of opportunities it represents and the regulatory challenges it poses. MSMEs typically lack knowledge on where their data would be most secure. This can make compliance to data localisation challenging, particularly for the more traditional MSMEs. However, the approach towards data storage and security among MSMEs in India is largely casual.

In view of this, stakeholders suggested that the government should give MSMEs sufficient time to understand, adopt and adapt to new policies. The government should disseminate information on regulatory changes more effectively. Often MSMEs are not aware of changes in regulations and might unwittingly end up on the wrong side of the law. Their costs might also suddenly increase if regulation requires them to migrate their data from overseas servers to those in India. Most MSMEs in our sample felt that apart from significant costs to their businesses, data localisation would not enhance data security as the physical location of data is immaterial to the security of data. One of the enterprises suggested that a more effective strategy to ensure security of data might be to assign a government body or agency to conduct an audit of the data management practices of enterprises operating in India.

Enterprises also expressed their concern about the poor data security infrastructure and ecosystem in India, improvement of which they believed, is a pre-requisite to any local data storage and management requirements. Stakeholders highlighted the advanced data storage ecosystems in other countries and the active contribution of those governments into creating it. Finally, data localisation and consequentially, migration of data to India from another country might entail a significant cost burden for MSMEs which might put their entire businesses at risk.

## 4. CONCLUSION AND POLICY RECOMMENDATIONS

There are two distinct sides to the data localisation debate in India – one that argues that data localisation will improve the security of citizen data, boost the domestic digital economy and make India the next big data hub; the other side argues that the costs to businesses arising from data localisation will far outweigh the benefits, will raise the cost of doing business in India and that unfettered government access to citizens' data raises questions about state surveillance and violation of privacy.

Several studies in the existing literature have attempted to quantify the economic costs of data localisation. The approaches and the overarching narrative have, however, focused mainly on the impact on big businesses. This study has attempted to estimate the regulatory burden on micro-small and medium-sized enterprises in India, arising from data localisation measures. MSMEs have been a key driver of growth for India's economy, contributing substantially to the country's GDP and employment. In recent years, the burgeoning number of startups, many of them with internet-based delivery models, has been India's innovation hotbed. The benefits and efficiencies accruing to MSMEs and startups from seamless flow of data across borders make them key stakeholders in the data localisation discourse. Therefore, it is essential that the impact of data localisation on the smaller enterprises is carefully estimated and understood and reflected in policy. It is critical that the implications of data localisation measures on MSME are taken into consideration by policy makers, especially because several other interventions are being put together by the government to boost MSMEs. For instance, credit delivery mechanisms are sought to be eased and interest rates lowered to encourage such enterprises.[74] It should not be the case that what the government gives with one hand, it takes away with another.[75] Small businesses and startups rely on cloud computing services, which saves them huge amounts of capital investment to buy computer hardware.[76] A 2015 study by the Leviathan Security Group finds that local companies would have to pay 30 – 60 percent more for their computing needs, in the event of a forced data localisation legislation. A consistent and integrated approach is essential if MSMEs are expected to play the role envisioned for them in the overall growth strategy.

The present study is, by its very nature, unable to study security considerations that have been invoked by the Sri Krishna Committee and others to justify data localisation. There is little publicly available data to scrutinise whether such a linkage is justified or whether data localization is an adequate and proportional response to privacy and security risks, if any of unfettered data transfer. We therefore focus on economic consequences of data localisation.

This study presents 10 use cases of MSMEs and MSME associations to provide a granular snapshot view of their data management practices, the regulatory challenges faced by them, the use of data in their business processes, quantum of cross-border data flows, impact of data localisation and their policy preferences. We find a mixed bag of responses – while some MSMEs report to be particularly vulnerable to data localisation, some others do not get impacted at all. It emerges that MSMEs might be less able to withstand costs of data localisation, as compared to bigger companies owing to economies of scale and bargaining power enjoyed by the latter. There is also a critical lack of awareness about policies surrounding data management and privacy in general, among MSMEs. Surprise implementation of regulations might

[74] See a list of government schemes for MSMEs here: https://msme.gov.in/all-schemes

[75] The Government of India has rolled out several schemes for the benefit of MSMEs (see footnote 73). For example, the Credit Guarantee Trust Fund for Micro and Small Enterprises, under which a collateral free loan up to a Rs.100 lakh limit is made available to individual enterprises on payment of a guarantee fee to the bank by the concerned enterprise.

[76] Justice B.N. Srikrishna Committee, "White Paper of the Committee of Experts on a Data Protection Framework for India" (2017)

have serious consequences for them in terms of shorter time windows for compliance. Higher compliance costs could make some MSMEs businesses commercially unviable. Moreover, lack of awareness regarding changes in regulations might inadvertently place them on the wrong side of the law. MSMEs have repeatedly stressed on the importance of improving the data storage ecosystem in India as a crucial pre-requisite before any measures of data localisation are enforced.

There is insufficient empirical data to arrive at a quantitative estimate for the impact of data localisation on MSMEs. However, our qualitative analysis provides some interesting insights. Through this study, we do not attempt to judge the efficacy of data localisation as a policy. The focus has been to bring out the challenges and opportunities, particularly in economic terms, which lie ahead for MSMEs in the event of a data localisation mandate in India. Following from the analysis presented in this study, we outline the following broad policy considerations that attempt to strike a balance between achieving the government's stated objectives and minimising the unintended consequences of data localisation.

**Increase awareness of MSMEs about data privacy and security** – the lack of awareness of MSMEs of the opportunities from and regulatory challenges posed by data-based businesses, are causes of concern. Governments can initiate public dissemination of such information for the benefit of MSMEs.

**Enhance access to and security of data storage infrastructure in India** – the cost of data storage appears to be higher in India as compared to alternative data server locations. Moreover, businesses typically seem to place less trust in the security provided by Indian data centres. Indian cloud service providers, do not yet provide several sophisticated services that global cloud service providers do.

**Provide a sufficient time window for smaller businesses to adapt to policy changes** – surprise implementations and consequently high compliance costs can make several MSMEs unviable. More lead time will allow them to plan ahead and spread out their costs.

**Consider data security audits and vulnerability assessments as an alternative to data localisation** – considering that one of the foremost objectives of data localisation is to secure citizens' data, rather than enforcing blanket data localisation, the government can instead consider security audits and vulnerability assessments of businesses, and undertake corrective measures accordingly.

**Data localisation might potentially hamper innovation** – small businesses, particularly startups have been the hotbed of innovation in India and across the world. They have devised innovative business models to provide services of value to individuals and the economy at large. Data localisation might also discourage foreign MSMEs to enter the Indian market- as the compliance costs would likely be unaffordable to them. In the long run, this is likely to hamper innovation in India and make the economy increasingly inward-looking.

**Economic benefits of data localisation are better realized through market mechanisms** - edge computing and the need for lower latency services is already encouraging players to store data closer to users' locations. Government and regulators can do much to remove existing barriers to investment in data centres. They could provide a mix of fiscal and other incentives to attract players to expand data centre infrastructure in India.

**Data localisation might risk picking winners in a competitive market** – the high ongoing compliance costs might force many MSMEs to shut shop, which will leave the market with only the relatively bigger sized enterprises which can afford to keep themselves afloat even in the face of additional recurring costs.

## 5. BIBLIOGRAPHY

**Annual Report**, *Ministry of Micro, Small and Medium Enterprises*, (2017 – 18)

**Bailey, Rishab, and Smriti Parsheera**. "Data localisation in India: Questioning the means and ends." *NIPFP Macro/Finance Group (forthcoming)* (2018).

**Brynjolfsson, Erik, Lorin M. Hitt, and Heekyung Hellen Kim.** "Strength in numbers: How does data-driven decision making affect firm performance?." *Available at SSRN 1819486* (2011).

**Castro, Daniel, and Alan McQuinn.** "Cross-border data flows enable growth in all industries." *Information Technology and Innovation Foundation* 2 (2015): 1-21.

**Chander, Anupam, and Uyên P. Lê.** "Data nationalism." *Emory LJ* 64 (2014): 677.

**Cory, Nigel.** "Cross-border data flows: Where are the barriers, and what do they cost?." *Information Technology and Innovation Foundation*, 2017.

**Ferracane, Martina.** "Restrictions on Cross-Border data flows: a taxonomy." (2017).

**Fraser, Erica.** "Data Localisation and the Balkanisation of the Internet." *SCRIPTed* 13 (2016): 359.

**Gurumurthy, Anita, Amrita Vasudevan, and Nandini Chami.** "The grand myth of cross-border data flows in trade deals." *IT for Change*, (2017)

**Hogan Lovells**, "Demystifying the U.S. CLOUD Act: Assessing the law's compatibility with international norms and the GDPR" (2019)

**IAMAI-IMRB**, "Digital Commerce Report" (2017)

**IDC**, "The Digitization of the World From Edge to Core" (2018)

**Justice B.N. Srikrishna Committee**, "White Paper of the Committee of Experts on a Data Protection Framework for India" (2017)

**Kong, Lingjie.** "Data protection and transborder data flow in the European and global context." *European Journal of International Law* 21, no. 2 (2010): 441-456.

**KPMG**, "Maharashtra and the exciting growth of its startup ecosystem" (2019)

**Kuner, Christopher.** "Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future." *OECD Digital Economy Papers*, 187, (2011)

**Leviathan Security Group** – Quantifying the Cost of Forced Localization (2015)

**Meltzer, Joshua P., and Peter Lovelock.** "Regulating for a digital economy: Understanding the importance of cross-border data flows in Asia." *Global Economy and Development Working Paper* 113 (2018).

**MIT Technology Review Custom + Oracle**, "The Rise of Data Capital"

**Nappinai, N. S.** "Cyber Crime Law in India: Has Law Kept Pace with Engineering Trends-An Empirical Study." *J. Int'l Com. L. & Tech.* 5 (2010): 22.

**OECD**, "Trade and cross-border data flows" (2018)

**Panday. Jyoti.** Rising Demands for Data Localization a Response to Weak Data Protection Mechanisms, Electronic Frontier Foundation (2017)

**Pepper, Robert, John Garrity, and Connie LaSalle.** "Cross-Border Data Flows, Digital Innovation, and Economic Growth." *The Global Information Technology Report 2016: Innovating in the Digital Economy* (2016): 39-40.

**Rubin, Ryan (2015).** "Companies should prepare for EU's forthcoming data protection regulation."

**Sadowski, Jathan.** "When data is capital: Datafication, accumulation, and extraction." *Big Data & Society* 6, no. 1 (2019): 2053951718820549.

**Stodden, Victoria.** "Enabling reproducibility in big data research: Balancing confidentiality and scientific transparency." *Privacy, Big Data, and the Public Good: Frameworks for Engagement* 1 (2014): 112-135.

**Strandburg, Katherine J.** "Monitoring, datafication and consent: legal approaches to privacy in the big data context." *Privacy, big data, and the public good: Frameworks for engagement* 1 (2014): 5-43.

**Telenor**, "Unleashing the benefits of free flow of data" (2018)

**The Centre for Internet and Society**, "The Localisation Gambit" (2019)

**Turner III, Daniel W.** "Qualitative interview design: A practical guide for novice investigators." *The qualitative report* 15, no. 3 (2010): 754-760.

**UNCTAD**, "Data protection regulations and international data flows" (2016)

**United States International Trade Commission (USITC)**, "Digital Trade in the U.S. and Global Economies", Part 1 (Washington, DC: USITC, July 2013)

**US Chamber of Commerce and Hunton & Williams (2014).** "Business without borders."

**World Trade Report**, The future of world trade: how digital technologies are transforming global commerce (2018)

**Data Sources**
TeleGeography

## 6. APPENDIX

Appendix 1: **Table A1.1:** Classification of MSMEs

| Manufacturing Sector | |
|---|---|
| Enterprise Category | Investment in Plant and Machinery |
| Micro enterprises | Does not exceed Rs. 25 lakh |
| Small enterprises | More than Rs. 25 lakh but does not exceed Rs. 5 crore |
| Medium enterprises | More than Rs. 5 crore but does not exceed Rs. 10 crore |
| **Service Sector** | |
| Micro enterprises | Does not exceed Rs. 10 lakh |
| Small enterprises | More than Rs. 10 lakh but does not exceed Rs. 2 crore |
| Medium enterprises | More than Rs. 2 crore but does not exceed Rs. 5 crore |

Appendix 2: **Table A2.1:** Summary of Case Study Findings

| Sector of Operation | Type of Organisation | Year of Incorporation | No. of Employees | Classification of Enterprise | Company Origin/ Headquarters | Country/ Countries of Operation | Data Storage | Cross-border Data Flow | Data Localisation in India | Data Localisation in Other Countries | Impact/ Potential Impact of Data Localisation in India |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Financial Services | Private | 2015 | 51-200 | Medium sized enterprise | India | India | All data stored in cloud using services provided by AWS. Data was relocated to Indian servers by AWS. | No | Compliant, as all data is stored in servers in India | Not applicable. | No impact, as all data is stored in India. |
| Education and Digital Marketing | Partnership | 2005 | 51-200 | Medium sized enterprise | India | Located in India, but has clients primarily in the United States. Their business model allows them to have clients across the world. | They currently store their data on Amazon's cloud in the US data centre. | Yes | Not compliant | Compliant with GDPR. | Potentially high impact. |
| IT Software and Service | Private | 2008 | 51 - 200 | Medium sized enterprise | India | Located in India, but has clients across the world, primarily in the United States. Their business model allows them to have clients across the world. | Stores data in AWS's data centre in North Virginia, USA | Yes | Not compliant | Compliant with GDPR. | Potentially high impact. |
| (SaaS) | | | | | | Has clients across the world, primarily in the United States. Their business model allows them to have clients across the world. | Data centre in North Virginia,USA | | | | |

| Sector of Operation | Type of Organisation | Year of Incorporation | No. of Employees | Classification of Enterprise | Company Origin/ Headquarters | Country/ Countries of Operation | Data Storage | Cross-border Data Flow | Data Localisation in India | Data Localisation in Other Countries | Impact/ Potential Impact of Data Localisation in India |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Education and networking | Private | 2015 | 11-50 | Small enterprise | India | India. Their users are spread across the world. | Data is stored on Amazon's cloud in its India data centre. |  | Compliant as all their data is stored in India. | They are GDPR compliant | No impact, as all data is stored in India. |
| Agriculture and Financial Services | Private | 2015 | 1-10 | Micro enterprise | India | India | Data is stored on cloud located in the US. | No | Stores personal data, which includes financial data, but not compliant with the RBI directive for local storage of payments data | Not applicable | No impact. |
| Research and Development | Private | 2012 | 7 on the job, also hires on contractual basis. | Micro enterprise | India | India | Data is stored in India. | No | Compliant as all data used for their work is stored in India and personal information of their employees stored in their own servers located in India. | Not applicable | No impact, as all data is stored in India |
| Digital Marketing and Software Products | Private | 2015 | 2-10 | Micro enterprise | India | Office located in India. Clients located in India and overseas. | Data stored on cloud in the US. | Yes | Not compliant | Compliant with GDPR and the California Privacy Act. | Potentially high impact. |
| Management Consulting and Marketing | Private | 2014 | 2 - 10 | Micro enterprise | United Kingdom | India and UK | Data stored on Dropbox, Boxcrypter on servers located either in the US or the EU. | Yes | Not compliant | Compliant with GDPR. | Potentially high impact. |

| Sector of Operation | Type of Organisation | Year of Incorporation | No. of Employees | Classification of Enterprise | Company Origin/ Headquarters | Country/ Countries of Operation | Data Storage | Cross-border Data Flow | Data Localisation in India | Data Localisation in Other Countries | Impact/Potential Impact of Data Localisation in India |
|---|---|---|---|---|---|---|---|---|---|---|---|
| MSME Association 1 | Not applicable | No information available | Not applicable | Not applicable | India | India | Not applicable | Not applicable | Not applicable | Not applicable | MSMEs have not adequately adopted digital technology and data usage. For those that use technology, they are unaware of the amount of data generated by their businesses. Potentially high impact on MSMEs that are data intensive, but the proportion of such enterprises is not very high. |
| MSME Association 2 | Not applicable | 2005 | Not applicable | Not applicable | India | India | Not applicable | Not applicable | Not applicable | Not applicable | They view the potential impact in terms of a sudden increase in costs because of data localisation laws. An estimate is that the cost of data storage in India is twice of that in USA. Views data localisation as an anti-trade measure. |