Data Flows and Data Localisation: An Economic Analysis

June 2020

INDIAN COUNCIL FOR RESEARCH ON INTERNATIONAL ECONOMIC RELATIONS

Data Flows and Data Localisation: An Economic Analysis

Kaushambi Bagchi

Gangesh Varma

Sashank Kapilavai

Table of Contents

List of Tables

List of Figures

Acknowledgment

We gratefully acknowledge the support from the Ministry of Electronics and Information Technology (MEITY) in facilitating this research under the Chair on Internet Policy. We humbly recognize the cooperation of the Joint Secretaries and Officers of the Internet Governance Division within MEITY, without whose constant support and diligence the research under this project would not have been possible. We also thank the Project Review & Steering Group (PRSG) for their valuable comments during the review meeting. With the unwieldy data work, we were also ably aided by our interns, Srishti Sinha, Shaivya Harit and Siddharth Mishra with infectious enthusiasm and utmost dedication. Last, but not least, we are grateful to all our colleagues at ICRIER for providing a stimulating environment that enriches our research. All errors are our own.

Executive Summary

Data forms the marrow of today's information society. Its creation and consumption continue to grow manifold and its flow between the innumerable nodes of individuals and machines fuels the digital economy.

Studies have shown that cross border data flows improve productivity and enable creation of efficient markets. According to McKinsey, all types of tangible and intangible flows have raised the world GDP by 10.1 percent, over the past decades. Data flows through the Internet, and other digital media, has become critically important to the information society and to the growth of the global economy. However, the rise of data flows is not an unmixed blessing. The ever more reliance on data as a fuel for growth raises concerns about the integrity of those using or having access to our personal data. Privacy as a fundamental right is being increasingly asserted as digital connectivity makes personal data vulnerable to actual and perceived misuse.

Amid these calls for concern, diverse data localisation measures have been resorted to by many countries. Data localisation has been defined differently in the nascent but growing literature on the subject and can be broadly characterized as any measure "that encumber(s) the transfer of data across national borders."

The dominant form of data localisation is localized data hosting, where governments compel Internet content hosts to store data of Internet users in the country on servers located within their jurisdiction. Within this type there are varying degrees of localisation. Some which allow for the data to flow outside of the geographic territory of the country as long as a copy of it is retained within the country's geographic territory (commonly referred to as *mirroring*). This copy may be live i.e. simultaneously updated with the original database or a periodically updated copy. A more strict degree of localisation mandates that data shall not leave the geographic territory of the country, and should be maintained, processed and analyzed only within. This is usually restricted to categories of data that are considered critical or highly sensitive.

Despite skepticism about the value generated by data localisation initiatives in domestic economies, several governments continue to adopt a range of data localisation laws to meet a variety of policy objectives, from safeguarding sovereignty, protecting data of individual citizens to promoting growth of the domestic digital economy. Some countries argue that limiting how personal data can be transferred across borders is the only practical way to protect privacy of their citizens, in the absence of a more comprehensive shared data protection regime between the countries concerned

The overarching objective of the study is to investigate whether there is a relationship between data regulation and localisation measures, and features of the economy (general and digital), and state capacity.

Towards this, measures of restrictions on cross-border data flows imposed by overarching data protection frameworks and sectoral legislations (General RCBDF and Sectoral RCBDF, respectively) for 74 countries are scored on the basis of types of restriction, type of data, and status of law. The computed scores are then correlated with a composite index, the 'Digital Potential Index' that captures the features of the General Economy, Digital Economy, and State Capacity of the 74 countries. These countries are also ranked based on the values of the Digital Potential Index. Furthermore, the scores that capture General RCBDF measures are correlated with the various sub-indices that capture the features of the economy and state capacity to observe more specific relationships subsumed under the composite index.

The results of the composite index show that India ranks 61 of the 74 countries: India ranks highly in the state-capacity sub index but features in the bottom 10 percentile in the index of digital economy and general economy. More generally, there is a weak negative, but statistically significant correlation between General RCBDF scores and the composite 'Digital Potential Index', as well as the sub-indices. The corresponding correlations of the composite index and sub-indices with Sectoral RCBDF scores are weak and statistically insignificant.

On the whole, correlations show that the higher a country ranks on the Digital Potential Index, i.e. the more developed the country is in terms of its general economy, digital economy, and state capacity, the less stringent restrictions it is likely to have on cross-border data flows. While the results seem to be general and intuitive, there remain gaps: for example, all the countries with the highest RCBDF score of 5, except for Pakistan, rank higher than India on the composite index, as well as the general economy and digital economy sub-indices, despite India having a lower RCBDF score. On the state capacity sub-index, however, India ranks higher than all these countries, except for Indonesia.

For a more in-depth and reflective understanding, case studies of specific data localisation measures by countries present a more nuanced picture of the global data localisation landscape. This paper conducts an in-depth review of four individual data localisation measures of Indonesia, Vietnam, Australia and South Korea. The key themes that emerge relate to:

Motivation and scope: Australia and South Korea both have very specific data localisation measures that motivated from concerns within specific sectors. Whereas the more recent localisation measures in Vietnam and Indonesia have much broader scope and are motivated by the protection of data privacy of citizens and easier access of data to law enforcement agencies within the country. However, there are also allied motivations that are not explicit such as greater control of online dissent or even the promotion of domestic industry.

Cost implications: The cost implications involved at a country level can be understood in two ways: first, the cost of required infrastructure and enabling environment; and second, the compliance costs to entities affected by the localisation measures. Data localisation measures are costly in terms of creating the infrastructural environment that enables data localisation, such as providing land, continuous power supply, cooling systems etc. Typical sources of

costs in complying with data protection regulations involve incident response plans, compliance audits and assessments, redress activities among others. The responses of countries to cost implications have been different. Vietnam proceeded with its legislation amid concerns of ambiguity and costs of compliance, but has subsequently planned to dilute the localisation requirements. Indonesia has introduced new provisions that ease its data localisation requirements.

Enforcement challenges and consequences: countries that introduced broad based data localisation requirements faced difficulties with compliance, followed by intense lobbying geared towards amending such requirements to more specific requirements. A major challenge in enforcing data localisation legislations is the formulation of the categories of data. In cases of both Indonesia and China, the initial legislation that mandated data localisation requirements were defined in ways that industry bodies in the respective countries found it ambiguous. South Korea's data localisation, witnessed success in terms of restricting location data within its borders through localisation measures. Consequently, the data localisation requirements compelled foreign companies to negotiate with South Korea for access to location, while ti also created competitive indigenous location-based industries.

Localisation norms in India already exist through different laws and policies, prior to the discussions in the Draft Personal Data Protection bill, 2018 and subsequently the Personal Data Protection Bill, 2019. The motivations for data localisation measures in India broadly stem from privacy, security and protectionist ends. RBI's data localisation directive in 2018 (now under review) cited security and monitoring as a key motivation, whereas, erstwhile data localisation measures within the draft National Policy Framework for E-Commerce in India were viewed as a measure to protect domestic companies including data centers and digital payments groups. India is at a crucial juncture with respect to its policies on data regulation. It presents a timely opportunity to examine the implications of data localisation measures, and potential impact it will have on the economic fabric in India.

Although data has been widely acknowledged to create economic value, its valuation has proven elusive as yet. As a result, economic impacts of data localisation measures, both at the micro and macro level are yet to be fully understood. This is due to the fact that many countries are at the stage of legislating, amending, or enforcing data localisation measures. In theory, the more restrictions placed on data, imply it could harm innovation and competition and thereby value. The inference from international comparisons based on derived indices shows that strength of a country's macroeconomic climate, digital economy and state capacity allows for a more permissive regime with respect to cross-border data flows. In the absence of explicit valuation models, this study presents case studies that review various data localisation measures, the reaction in countries, and the implication and challenges that follow from such measures. These present considerations that inform the utility of data localisation measures beyond those used in construction of the index. Additional considerations that emerge include *regulatory impact assessment, specificity of data localisation measures, coordinated strategies towards data localisation measures, requisite regulatory environment, and fixing liability and burden of costs.*

Data Flows and Data Localisation: An Economic Analysis

"It is not the amount of knowledge that makes a brain. It is not even the distribution of knowledge. It is the interconnectedness"

- James Gleick, The Information: A History, A Theory, A Flood.

1. Introduction

The ubiquity of data and its importance has been made more apparent than ever by the advancement of technology. Human activity has undergone 'datafication' in many aspects – social, political and economic. The Economist magazine declared that *data* has replaced *oil* as the most valuable resource in the world.[1] Businesses are becoming progressively reliant on data for activities like monitoring production systems, managing a global workforce, and managing supply chains.[2] The troves of data generated by and flowing between the innumerable nodes of digitally connected individuals and machines are both the foundation and fuel of the digital economy.

The reasons data inspires improvements in efficiency are not hard to discover. Decisions of firms and individuals made with limited information are bound to be suboptimal compared to those made with technology enabled access to data and information. More than a century ago Sir Arthur Conan Doyle expressively declared *"It is a capital mistake to theorize before one has data*".[3] A 2016 study by McKinsey argued that cross border data flows improve productivity and enable creation of efficient markets. It stated that cross-border Internet bandwidth had grown 45 times since 2005 and is projected to increase by another nine times in the following five years, as data traffic between and within companies expands. According to McKinsey Global Institute (MGI), all types of tangible and intangible flows have raised the world GDP by 10.1 percent, over a decade i.e. from 2003 to 2013. This value amounted to US$7.8 trillion in 2014, of which, data flows accounted for US$ 2.8 trillion-an astounding 36 percent. According to Telegeography, in 2019, global internet bandwidth increased by 26 percent, and at a compound annual growth rate of 28 percent between 2015 and 2019.[4] Regionally, Africa led the pack in the growth of international internet bandwidth at a CAGR of 45 percent between 2015 and 2019, followed by Asia at a CAGR of 42 percent over the same time period.[5] Information that flows through the Internet, or digital data, is critically important to society and to the growth of the global economy.

Alas, exploding data flows are not an unmixed blessing. The ever more reliance on data as a fuel for growth also raises concerns about the integrity of use of personal data. Privacy as a fundamental right is being increasingly asserted as digital connectivity makes personal data

---

1 The Economist, May 2017, https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data
2 Cory (2017)
3 Arthur Conan Doyle (1891) *A Scandal in Bohemia*
4 'The State of the Network 2020 Edition', *Telegeography*
5 Ibid

vulnerable to actual and perceived misuse. Online service providers (OSPs) such as Facebook, Twitter, Dropbox, Yahoo etc. play a crucial role in shaping the informational environment and influence users' experiences and interactions within it.[6] OSPs are often seen as information gatekeepers[7], for they control the information available online[8] thus drawing attention to their public role in contemporary societies. Their moral responsibilities include issues concerning freedom of speech, censorship and privacy.[9]

Notwithstanding the associated complexities, the increasing use and value of data has triggered a passionate discourse around protection and privacy. The Internet, while protected is also a vulnerable space. Incidents of cyber-attacks have become commonplace. Data released by a social media metrics company called NewsWhip found that 'high quality' news sources were getting less engagement on Facebook and 'lower quality' sites were getting a lot more.[10] In the first half of 2019, data breaches exposed 4.1 billion records.[11] Cybercrime damages are likely to reach USD 6 trillion in 2021.[12] From the long list of cyberattacks and data breaches[13], the infamous Facebook - Cambridge Analytica data scam, most notably shook the collective consciousness of our perpetually logged in lot. We are perhaps exercising a bit more caution with regard to the amount of information we share about ourselves on the Internet. However, the best of us continue to remain in the dark about the amount of our data that is actually on the web, and more importantly, how much of it is secure. In light of the importance of data, and its regulation in the digital economy, it is important to understand and closely examine the emerging regulatory landscape that would be the foundation of the future development of the data economy.

This paper focuses on the correlation between data localisation measures and other indicators of the economy including state capacity with a view to unpick patterns, if any, between economic development and type of localisation measures introduced across countries. The next section defines data localisation, outlines its principal motivations and provides a summary of data protection regulations in India. Section 3 develops a score (index) of restrictions to cross-border data flows to rank countries and also constructs an index consisting of three sub-indices that relate to the general economy, the digital economy, and state capacity. Section 4 gleans insights from laws surrounding data protection and restrictions on cross-border data flows spawning four different countries with decidedly different approaches to data governance. Section 5 concludes.

2. Defining Data Localisation

Data localisation has been defined variously in the nascent but growing literature on the subject and can be broadly characterized as any measure "that encumber(s) the transfer of

6 Taddeo and Floridi. (2016)
7 Calhoun, C. J. (2002).
8 Shapiro (2000), Hinman (2005), Laidlaw (2008)
9 Op cit, 3
10 https://www.cjr.org/the_new_gatekeepers/facebook-algorithm-quality-news.php
11 https://www.varonis.com/blog/cybersecurity-statistics/
12 'The Global Risks Report 2020', *World Economic Forum*
13 https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents

data across national borders".[14] Corresponding to this are two 'default positions', one which presumes that data flows are permissible with attendant regulation, and the other which presumes that data flows, specifically personal data, are not permissible without a legal basis.[15]

Implementation of data localisation measures usually takes two distinct routes[16]

a) ***Localised Data Hosting*** **-** a policy whereby national governments compel Internet content hosts to store data on Internet users in the country on servers located within the jurisdiction of the government.

b) ***Localised Data Routing*** **-** a policy whereby national governments compel Internet service providers to route data packets sent between Internet users located in their jurisdiction across networks located only within their jurisdiction.

The dominant form of data localisation is localized data hosting. Within this type there are varying degrees of localisation. Some which allow for the data to flow outside of the geographic territory of the country as long as a copy of it is retained within the country's geographic territory (commonly referred to as mirroring). This copy may be live i.e. simultaneously updated with the original database or a periodically updated copy. A stricter degree of localisation mandates that data shall not leave the geographic territory of the country, and should be maintained, processed and analyzed only within. This is usually restricted to categories of data that are considered critical or highly sensitive.

The information sharing and Internet regulation narrative has gradually shifted from efforts to prevent data from flowing into a country through censorship, to include efforts to prevent data from flowing out through data localisation.[17] The issue assumes significance because the future of global trade is inextricably linked to the nature of localisation measures that emerge in an increasingly digitised world. Due to the pervasive nature of data, its security is constantly threatened and evidence of breaches add to the risk perception. Data localisation is a measure introduced to gain control over data belonging to citizens and residents to secure critical interests of the nation state.[18]

2.1 Motivations for Data Localisation

The Edward Snowden episode of 2013 marks a watershed in the discourse on location of digital data. Efforts to keep data within the territorial jurisdiction have gained more salience in the wake of rising evidence of widespread electronic spying. Despite skepticism about the value generated by data localisation initiatives in domestic economies,[19] several governments

---

14 Chander and Lê (2014)
15 Kuner (2011)
16 Selby (2017)
17 Ibid
18 http://www.mondaq.com/india/x/736934/Data+Protection+Privacy/The+Debate+Data+Localisation+And+Its+Efficacy
19 Baeur et al, 2014

continue to adopt a range of data localisation laws to meet a variety of policy objectives, from safeguarding sovereignty, protecting data of individual citizens to promoting growth of the domestic digital economy.[20] In some cases local law enforcement agencies press for personal data to be stored locally in order to easily access data for crime detection rather than waiting for responses to requests made to foreign entities which store data abroad.[21] The vulnerability of an overwhelming reliance on fibre optic cable networks that are used to transmit data across countries also has a bearing on the need for some countries to enforce data localisation norms.[22] In the post-Snowden era, the fear of foreign surveillance has been reinforced, motivating nations to explore local storage and processing of critical data as a means to preserve national interest.[23] The demand for localisation is thus driven by various factors ranging from protection of individual rights, law enforcement challenges, security, to an inward outlook on commerce, etc.[24] Some countries argue that limiting how personal data can be transferred across borders is the only practical way to protect privacy of their citizens, in the absence of a more comprehensive shared data protection regime between the countries concerned.[25]

Data localisation thus can and indeed has been justified on several grounds. There are however differences in the way countries have chosen to localize, the regulatory measures rooted in their legal traditions and cultures.[26] For example, GDPR in the EU are much more prescriptive in their application compared to the US rules on data protection. Individual country policies on data localisation can thus be broad or narrow in scope, explicitly required by a specific law or be the de facto aggregation of other restrictive policies. The latter could include rules that make it infeasible or hard to transfer data, such as requiring companies to store a copy of the data locally, requiring companies to process data locally, or mandating individual or government consent for data transfers across borders.

From an economic perspective, the narrative driving localisation efforts is a desire to attract investment, fuel innovation and create competitive advantage for local companies.[27] A nation's ability to control data flows also has implications for global Internet governance rankings. The trade off to data localisation efforts come in the form barriers to digital trade. Such services trade from the territory of one country into the territory of another through the telecommunications and Internet infrastructure will be the most impacted. Cutting off data flows or making such flows harder or more expensive puts foreign firms at a disadvantage[28] while also making it challenging for local companies to participate in the global digital

[20] Chander and Le (2014); Castro and Mcquinn (2015); US Chamber of Commerce and Hunton & Williams (2014)
[21] Op cit, 3
[22] Ibid
[23] Bauer et al. (2013, 2014 & 2015)
[24] Chander and Le (2014); Castro and McQuinn (2015); US Chamber of Commerce; Hunton & Williams (2014); Kuner (2011)
[25] See: https://www.eff.org/deeplinks/2017/08/rising-demands-data-localisation-response-weak-data-protection-mechanisms
[26] Op cit, 2
[27] Kathuria et al. (2019)
[28] USITC (2017)

economy.[29] A policy choice on data localisation would consider these trade-offs, including the possibility of retaliatory measures from partner countries.

The two major driving forces behind legislation on data localisation – data protection considerations including privacy and its alter ego, security and economic considerations – are either explicitly given by the state as the rationale or implied through its regulatory devices. The following section provides a brief overview of the global trends in the development of data localisation policies.

2.2 Landscape of Data Localisation Measures

There is variety in the form that data localisation takes by targeting certain types of data or sectors or both. Appendix 1 presents a snapshot of data localisation measures globally, the current status and other details.

Type of data localisation measures

At one end of the spectrum of data localisation is the imposing of conditions for cross border data flows to completely restricting any transfer of data beyond the geographic territory of the country at the other. In between are mandates for local processing and local storage. Regulatory instruments can use any one or a combination or all of these measures to control data flows. According to Ferracane (2017), 42% of restrictions impose conditions on cross border data flows, while 33% mandate local processing requirements or complete ban on flows outside and 25% are local storage requirements.[30]

Types of data localized:

Majority of data localisation measures across the world target personal data. Some key types of data subject to localisation mandates include financial data, health data, and business records. At the same time, the taxonomy is not watertight since there are considerable overlaps between different types of data such as between personal data and financial data. Furthermore, some countries have different levels of localisation mandates across categories. In some regulations, strategic or critical personal data is often prescribed to be localised completely i.e. not allowed to flow outside the geographic boundaries of the country.

Scope of data localisation measures:

Data localisation measures also vary in scope. Some are restricted to specific sectors, while others cut across sectors across a broad horizon. Some of the key sectors that have seen data localisation mandates are the financial sector and the health sector, followed by geolocation services. Personal data protection usually manifests in broad regulations that are not sector specific. However, most broad-based regulations do not mandate complete ban on transfer

[29] IAMAI (2016); UNCTAD (2016)
[30] Ferracane (2017)

but require fulfillment of conditions that ensure adequate levels of protection for transfer of data to be allowed.

Most studies that examine implications of data localisation measures assume one of two things: either the irrelevance of the economic costs of localisation measures[31] or doubt the ability of achieving the purported objectives through alternative means such as trade agreements or domestic policy instruments[32]. If economic costs are irrelevant or not accounted for in the policy decision to impose localisation, and other instruments are allegedly ineffective, the question naturally arises if state capacity is adequate to enforce data localisation measures. This is the line of inquiry in the next section.

2.3 Data Protection and Localisation in India

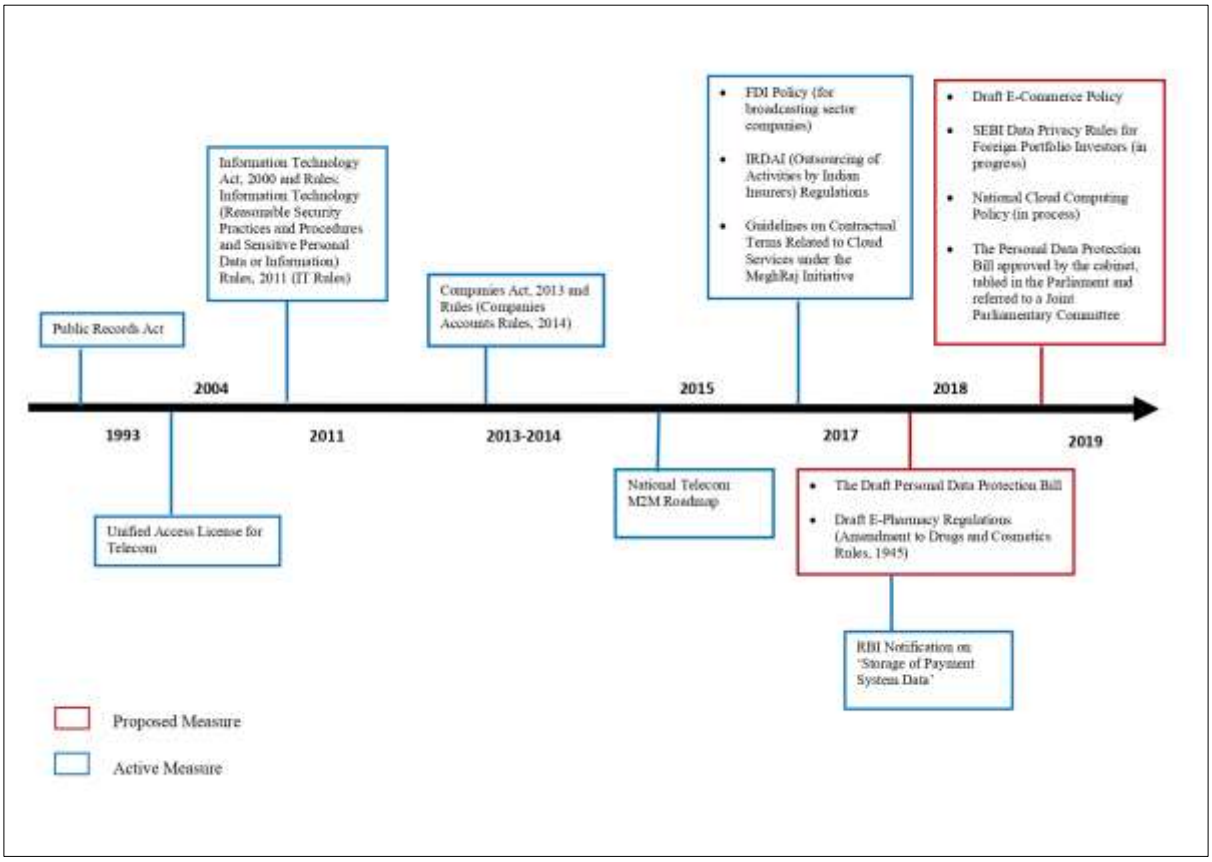
Debate and discourse on data localisation in India has gained momentum over the last couple of years. Some of the earliest examples of regulations adopted to secure sensitive data are the Public Records Act (1993) and security conditions under the Unified Access License for Telecom Services (2004). Under the Public Records Act (1993), transfer of public records outside the Indian territory is prohibited unless such transfer is for an official purpose or with permission from the central government.[33]

In India, even in the absence of an exclusive law on data protection and privacy, cross-border data flows have been regulated either implicitly or explicitly by several sectoral policies. Examples include telecommunications and internet service providers who are holders of the Unified Access License. These entities are prohibited from transferring user information and any accounting information related to subscribers, except for international billing to any person or place outside India.[34] Rules under the IT Act (2000) limit transfer of sensitive personal data by a body corporate to another entity or person, within or outside India, under the condition that the other person/ entity will be able to provide the same level of data protection that is expected under the IT rules. such transfers are permitted only if considered necessary for the performance of an existing contract and if the person providing the information has consented to it.[35,36] For entities in the purview of the Companies Act (2013), a back-up of books of accounts and other books and papers of the company that are maintained in an electronic mode, including any records that are kept outside India, must be periodically stored in servers physically located in India.[37,38] Figure 2.1 presents a timeline of laws surrounding data regulation in India.

---

31 Bauer (2014), Cory (2017)
32 Aaronson (2016)
33 See Section 4 of the Public Records Act 1993
34 Bailey and Parsheera (2018)
35 *Ibid*; https://www.ikigailaw.com/data-localisation-requirements-for-telecom-and-internet-service-providers-current-law/#acceptLicense
36 Kathuria et al. (2019)
37 "The Localisation Gambit". *The Centre for Internet and Society* (2019)
38 Op cit, 36

Figure 2.1: Timeline of Data Regulation Policies in India



Source: Compiled by authors

The Personal Data Protection Bill

The Justice Srikrishna Committee Report and subsequently the Draft Personal Data Protection Bill 2018, along with sectoral regulations such as the RBI's directive on local storage of payments data and the (now erstwhile) data localisation requirements in the draft national e-commerce policy, prompted most of the ongoing discussion around data localisation in India. The Personal Data Protection Bill, 2019 was approved by the cabinet and tabled in the parliament in December 2019. It was, thereafter, referred to a Joint Parliamentary Committee appointed by the Government of India.[39]

The current version of the bill has undergone several changes from its draft version.[40,41] Among them, some notable departures from its draft version are as follows:[42,43]

(i) Whereas the draft had said that all data fiduciaries needed to store a copy of all personal data in India, the approved bill dilutes this requirement, by mandating individual

39 https://www.medianama.com/2020/02/223-joint-parliamentary-committee-consultation-pdp-bill-2019/
40 https://sflc.in/key-changes-personal-data-protection-bill-2019-srikrishna-committee-draft
41 For the most recent version of the bill, see: http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf
42 https://indianexpress.com/article/explained/personal-data-protection-bill-cyber-security-hacking-6153015/
43 Op cit, 40

consent for cross-border data transfers. The bill, however, still requires that all sensitive personal data be stored in India. Such data can be transferred and processed only under certain conditions, including but not limited to, explicit individual consent and approval from a Data Protection Authority (DPA). Critical personal data must be stored and processed in India. Transfers of critical personal data may be allowed for emergency purposes upon approval by the central government.

(ii) Provision of non-personal data to the government on demand is mandatory for data fiduciaries, as per the bill. Non-personal data refers to anonymised data, such as traffic patterns or demographic data, typically used by companies to fund their business models. Non-personal data did not come under the purview of the draft bill.

(iii) Social media companies are required by the bill to develop their own user verification mechanism. Such companies are deemed significant data fiduciaries, in consideration of the large volume and high sensitivity of data handled by them.

(iv) The draft bill classified data into three categories – personal data, sensitive personal data and critical personal data. The first two types can collectively include employee personal data, transaction and payments related data, photos and potential biometric data, passwords, data related to personal correspondence, non-differential client data that is encrypted and stored in servers, geo-location data, etc. The draft bill did not define the third type i.e. critical personal data. This definitional ambiguity is retained in the current version of the bill. However, the ambit of personal data has been expanded to include inferred data for profiling purposes. Passwords have been declassified as sensitive personal data. Most importantly, critical personal data remains undefined and the government can at any point deem something to be critical, such as military or data related to national security.

A robust overarching framework that provides guidelines to safeguard privacy is presently of utmost importance. In India, however, the sequence was reversed with sectoral regulation preceding the overarching privacy law. Laws implemented in initial haste such as RBI's guidelines on the localisation of payments data and the first draft of the national e-commerce policy created significant chaos in the industry and affected business sentiments. Such regulations have often overlapped with existing policies, resulting in regulatory overreach and uncertainty.

3. Digital Economies and State Capacity

3.1 Internet with Borders

Cross border implications of domestic policy action been a subject of raging debate in the G20 especially after the global financial crisis of 2008. The necessity of policy coordination has become paramount. With Internet cutting across territorial borders, local laws cease to be applicable on geographic boundaries.[44] Indeed, the absence of borders is one of the most

[44] Johnson and Post (1996)

attractive aspects of the Internet, thus making policy coordination a *sine qua non* in this space. Instead, borders are being created in cyberspace as in the physical world, being manifested in the various forms of data localisation observable globally. The relationship between the depth of data localisation and state capacity is explored in the next section.

3.2 State Capacity

From the time of Adam Smith (1776), the role of the state has been a crucial determinant of the relative wealth of nations.[45] State capacity can be broadly defined as the institutional capability of the state to implement its policies that raise collective welfare.[46] It constitutes both fiscal and legal capacity.[47] The importance of state capacity in supporting economic development is well established in both the political science and economics literature. Besides state capacity, other factors associated with a policy of data localisation could be economic attainment and digital prowess.

3.3 Digital Potential Index

The overarching objective of the study is to investigate the correlation between data localisation measures and other indicators of the economy including state capacity with a view to unpick patterns, if any, between economic development and type of localisation measures introduced across countries. Accordingly, an index is developed for each of General Economy, Digital Economy and State Capacity for a set of 74 countries. Each Sub-Index consists of several variables as shown in the table below and is computed using the standard min-max transformation to normalise values between 0 and 1, the higher numerical value reflecting better performance. A composite index, which we call the 'Digital Potential Index' is computed from the sub-indices using a simple aggregation technique. In addition, scores are computed for data localisation. Appendix 2 provides the complete data set with sources and the detailed methodology.

Table 3.1: List of Indicators

General Economy Sub-Index	Digital Economy Sub-Index	State Capacity Sub-Index
1. Income Level 2. GDP Per Capita (PPP, Current International $) 3. Unemployment Rate (% of Total Labour Force) 4. Current Account Balance (% of GDP) 5. Foreign Direct Investment, net inflows (% of GDP)	1. International Internet Bandwidth per Internet User (Mbit/s) 2. Percentage of Individuals Using the Internet 3. Fixed Broadband Subscriptions per 100 Population 4. Mobile Cellular Subscription per 100 Population 5. Mobile Broadband Subscribers per 100 Population 6. Secure Internet Servers (per 1 Million People)	1. Government Net Lending/ Borrowing (% of GDP) 2. Regime Type 3. Political Stability and Absence of Violence 4. Government Effectiveness 5. Regulatory Quality 6. Rule of Law 7. Control of Corruption

[45] Acemoglu and Robinson (2012)
[46] Besley and Persson (2011)
[47] Ibid

Establishing a quantitative association between data localisation and key national characteristics namely general economy, digital development and state capacity is a first step in the attempt to understand whether such linkages exist in practice. The general economy sub index is a proxy for level of economic development and openness, the digital economy sub index captures the extent of digitization while the state capacity index is an estimate for legal and fiscal capacity of the state. In theory, all three sub-indices jointly and severally, should be inversely related to data localisation efforts. For example, the higher the levels of income and openness, the less likely are countries to pursue data localisation initiatives, all else remaining constant. Similarly, for digital economy and state capacity. Since data localisation is a recent phenomenon, there is no clear empirical evidence on the relationship between macroeconomic characteristics (income level, GDP per capita, trade balance etc.), digital economy characteristics (international internet bandwidth per Internet user, internet penetration measures etc.) and state capacity characteristics (political stability and absence of violence, regulatory environment, control of corruption etc.) individually and collectively. Thus, this may be regarded as a first serious attempt to isolate such correlations. Table 3.2 below provides the consolidated results of the sub-indices and the Digital Potential Index (DPI). The rankings are listed below alongside each sub-index, and the composite value of the sub-indices is reflected in the ranking alongside the Digital Potential Index.

Table 3.2: Digital Potential Index – Results and Rankings

Country	General Economy Sub-Index (0-1)	Rank	Digital Economy Sub-Index (0-1)	Rank	State Capacity Sub-Index (0-1)	Rank	Digital Potential Index (0-1)	Rank
Singapore	0.788	1	0.667	3	0.882	5	0.779	1
Luxembourg	0.693	3	0.716	2	0.893	3	0.767	2
Denmark	0.628	11	0.725	1	0.854	9	0.736	3
Switzerland	0.624	13	0.615	5	0.889	4	0.709	4
Sweden	0.638	10	0.555	10	0.869	7	0.688	5
Ireland	0.728	2	0.520	16	0.810	12	0.686	6
Finland	0.605	19	0.578	8	0.874	6	0.685	7
Netherlands	0.543	39	0.641	4	0.864	8	0.683	8
Norway	0.602	20	0.514	17	0.920	1	0.679	9
Germany	0.623	14	0.556	9	0.830	10	0.670	10
New Zealand	0.578	32	0.523	15	0.893	2	0.665	11
Australia	0.621	15	0.537	13	0.819	11	0.659	12
Estonia	0.591	25	0.602	6	0.706	18	0.633	13
UK	0.587	29	0.526	14	0.778	14	0.630	14
USA	0.618	17	0.596	7	0.671	23	0.628	15
Canada	0.612	18	0.468	24	0.803	13	0.627	16
Japan	0.582	30	0.546	11	0.747	15	0.625	17
France	0.626	12	0.491	19	0.727	16	0.615	18
South Korea	0.599	21	0.539	12	0.694	19	0.611	19
Cyprus	0.649	8	0.502	18	0.663	24	0.605	20
Spain	0.672	5	0.460	26	0.656	26	0.596	21
Uruguay	0.594	23	0.472	22	0.691	20	0.586	22
Portugal	0.597	22	0.429	35	0.724	17	0.583	23
Qatar	0.686	4	0.447	29	0.591	33	0.575	24
Czech Republic	0.576	35	0.472	23	0.676	22	0.575	25
Belgium	0.578	33	0.451	28	0.686	21	0.572	26

Country	General Economy Sub-Index (0-1)	Rank	Digital Economy Sub-Index (0-1)	Rank	State Capacity Sub-Index (0-1)	Rank	Digital Potential Index (0-1)	Rank
Latvia	0.589	27	0.460	25	0.644	27	0.565	27
Slovenia	0.592	24	0.441	30	0.658	25	0.564	28
Poland	0.581	31	0.485	20	0.602	31	0.556	29
Slovakia	0.589	28	0.440	31	0.606	30	0.545	30
Italy	0.644	9	0.439	33	0.542	36	0.542	31
Costa Rica	0.543	38	0.456	27	0.611	29	0.537	32
Greece	0.651	7	0.408	37	0.496	38	0.519	33
Malaysia	0.505	43	0.398	40	0.611	28	0.505	34
Bulgaria	0.499	44	0.440	32	0.548	35	0.496	35
South Africa	0.652	6	0.338	44	0.441	44	0.477	36
Hungary	0.433	55	0.378	41	0.598	32	0.470	37
Saudi Arabia	0.619	16	0.418	36	0.356	56	0.464	38
Romania	0.495	45	0.399	39	0.484	39	0.460	39
Thailand	0.484	50	0.403	38	0.482	40	0.456	40
Bahrain	0.553	36	0.480	21	0.331	59	0.454	41
Namibia	0.589	26	0.203	61	0.524	37	0.439	42
Colombia	0.522	41	0.296	48	0.465	41	0.428	43
Brazil	0.545	37	0.327	46	0.393	52	0.422	44
Turkey	0.577	34	0.312	47	0.355	57	0.415	45
Russian Federation	0.510	42	0.436	34	0.292	65	0.412	46
Kazakhstan	0.489	48	0.370	43	0.365	55	0.408	47
Jordan	0.541	40	0.286	50	0.394	51	0.407	48
China	0.491	47	0.371	42	0.340	58	0.400	49
Mexico	0.488	49	0.279	52	0.420	48	0.396	50
Bhutan	0.339	69	0.230	58	0.562	34	0.377	51
Indonesia	0.414	58	0.257	55	0.456	42	0.376	52
Paraguay	0.481	51	0.236	57	0.408	50	0.375	53
Philippines	0.391	64	0.284	51	0.430	46	0.369	54
Vietnam	0.405	60	0.330	45	0.366	54	0.367	55
Ghana	0.399	62	0.251	56	0.445	43	0.365	56
Sri Lanka	0.473	52	0.189	64	0.428	47	0.363	57
Morocco	0.428	56	0.269	53	0.386	53	0.361	58
Ukraine	0.439	54	0.288	49	0.274	67	0.334	59
Algeria	0.495	46	0.258	54	0.224	70	0.326	60
India	0.412	59	0.109	68	0.440	45	0.320	61
Bolivia	0.391	65	0.224	59	0.302	64	0.305	62
Egypt	0.455	53	0.198	62	0.242	68	0.298	63
Kenya	0.381	67	0.112	67	0.313	62	0.269	64
Nepal	0.289	72	0.206	60	0.305	63	0.267	65
Bangladesh	0.393	63	0.126	65	0.276	66	0.265	66
Myanmar	0.378	68	0.195	63	0.219	71	0.264	67
Rwanda	0.274	73	0.089	69	0.417	49	0.260	68
Nigeria	0.421	57	0.114	66	0.211	73	0.249	69
Pakistan	0.402	61	0.061	70	0.232	69	0.232	70
Uganda	0.302	70	0.053	71	0.323	61	0.226	71
Malawi	0.299	71	0.012	74	0.324	60	0.212	72
Afghanistan	0.387	66	0.026	73	0.085	74	0.166	73
Mozambique	0.208	74	0.032	72	0.217	72	0.153	74

Source: Author's calculations

The results show that India ranks 61 of 74 countries in terms of the Digital Potential Index. India performs the best in the state capacity sub index but is in the bottom fifteen percentile in the other 2 sub-indices namely digital economy and general economy (See Table 3.2) We check the robustness of the Digital Potential Index by comparing it with globally recognised indices, such as – Global Cybersecurity Index 2018, Network Readiness Index 2019, Global Innovation Index 2019 and Doing Business Index 2020. The correlation matrix is given below.

Table 3.3: Correlation Matrix – Digital Potential Index, GCI, NRI, GII and DBI

Correlation Matrix	Digital Potential Index	General Economy Sub-Index	Digital Economy Sub-Index	State Capacity Sub-Index
Global Cybersecurity Index	0.6564*	0.5922*	0.6603*	0.5867*
Network Readiness Index	0.9521*	0.7932*	0.9373*	0.898*
Global Innovation Index	0.7883*	0.6471*	0.7631*	0.7616*
Doing Business Index	0.743*	0.5841*	0.737*	0.7193*
(*) indicates significance at 5% level				

Source: Author's calculations

The correlation results show that the Digital Potential Index as well as the sub-indices are (statistically) significantly correlated with the all four global indices. The highest correlation is with the Network Readiness Index (NRI). This could be due to the fact that both the NRI and the Digital Potential Index use a number of digital economy variables as the building blocks for the index. The results show that our indices are quantitatively robust and qualitatively aligned with the global indices.

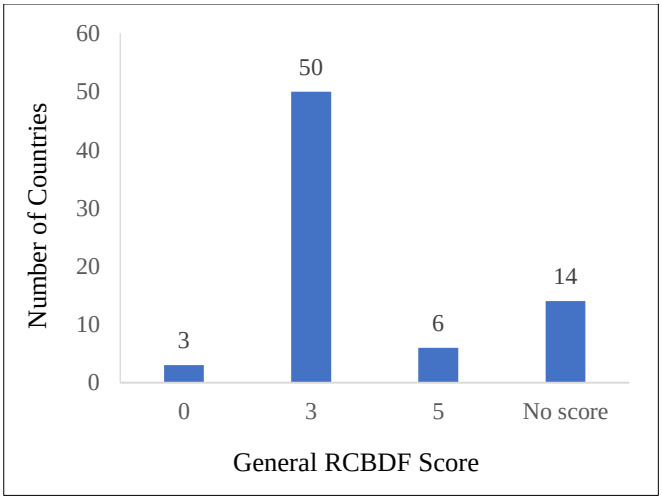
The more important question however, is the correlation of each index with data localisation, or more specifically, restrictions to cross-border data flows (RCBDF). In the empirical literature, data localisation is graded either by the type of data localised, by the strength of data localisation, or by the number of laws that encumber cross border data flows, but no comprehensive quantification of data localisation exists. In this study, we attempt to arrive at a score for data localisation for countries, drawing from the classification by ITIF[48], Ferracane (2017) and ICRIER's existing body of work on cross-border data flows. We develop two different sets of scores – one based on restrictions to cross-border data flows in overarching data protection laws (General RCBDF) and another based on such restrictions in sectoral data protection laws (Sectoral RCBDF). For General RCBDF scores, each country is scored on the basis of three parameters – type of restriction (unconditional flow, conditional flow without local storage, mirroring, conditional flow with local storage, ban on transfer), type of data (sensitive personal data, personal data, non-personal data, all types of data) and status of law (proposed, effective). For Sectoral RCBDF scores, each country was scored on the basis of – number of sectors (none, one, multiple), type of restriction (unconditional flow,

[48] https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost

conditional flow without local storage, mirroring, conditional flow with local storage, ban on transfer) and status of law (proposed, active).

The next graph reports the General RCBDF scores measured across countries. The scores vary between 0 and 5, a higher value indicating stronger restrictions (or potential restrictions) to cross-border data flows. Figure 3.1 below gives the number of countries, from our set of 74 countries that have General RCBDF scores in the calculated range. No score has been assigned to countries that do not have an overarching data protection law and there is no clear information available on restrictions to data flows imposed by other existing laws, countries for which no clear information is available for any data related regulations, and for countries which have draft policies for data protection and privacy in place but information on restrictions to cross-border data flows are either not clear in the draft legislation, or not available and information on restrictions imposed explicitly by any other existing regulations are either unclear or unavailable. A score of zero has been assigned to countries where there are existing or proposed data protection legislations where it can be clearly inferred that unconditional flow have been granted to cross-border data. As can be observed in the figure below, such cases are far and few in our set of 74 countries. More details on the methodology and country wise scores for both General and Sectoral RCBDF are provided in Appendix 2.

Figure 3.1: Number of Countries with General RCBDF Scores from 0-5



Source: Authors' calculations

It is worth noting here that among countries with draft or proposed legislations, only India and Pakistan have been assigned a General RCBDF score. The draft data protection bills of both countries are similar on several fronts, including the classification of data into personal, sensitive personal and critical personal data types, with critical personal data being undefined and left to the discretion of the central government and local storage requirements for sensitive personal data, among others.[49] Additionally, while India's current PDP Bill, 2019

[49] https://www.natlawreview.com/article/pakistan-introduces-new-draft-personal-data-protection-bill#:~:text=In%20addition%2C%20under%20the%20Bill,authority%20to%20enforce%20the%20act.&text

has removed mirroring requirements in a departure from its draft, Pakistan's draft legislation includes mirroring requirements.[50] That is the sole parameter that assigns a slightly higher score of 5 to Pakistan (numerically, at par with the likes of China and Russia) and a lower score of 4 to India.[51] However, Pakistan's stringency of restrictions of cross-border data flows is a potential occurrence at the time that this report is being written. While India's PDP Bill is not yet active, there are existing regulations under the IT Act that impose restrictions to cross-border data transfers. Therefore, India's legislative stringency is more active than proposed. The RCBDF scoring, evidently, does not account for these nuances. However, these scores can be considered as indicative of a country's overall approach to data protection and privacy, particularly in context of cross-border data flows.

In the next step, correlations are estimated between the Digital Potential Index and the sub-indices with the General RCBDF scores for all 74 countries. We estimate both Pearson's correlation as well as Spearman's rank correlation[52]. For countries with scores in the range of 0 to 5 i.e. with and without restrictions to cross-border data flows, the General RCBDF scores are negatively correlated with the Digital Potential Index and all three sub-indices. These correlations are weak. However, the Pearson's correlation estimates are statistically significant for the DPI and the State Capacity Sub-Index. The Spearman's rank correlation estimates are all statistically significant.[53] Figure 3.2 provides a graphical representation of Pearson's correlation estimates.

=Data%20Localization%3A%20Critical%20personal%20data,data%20centers%20located%20in%20Pakistan.

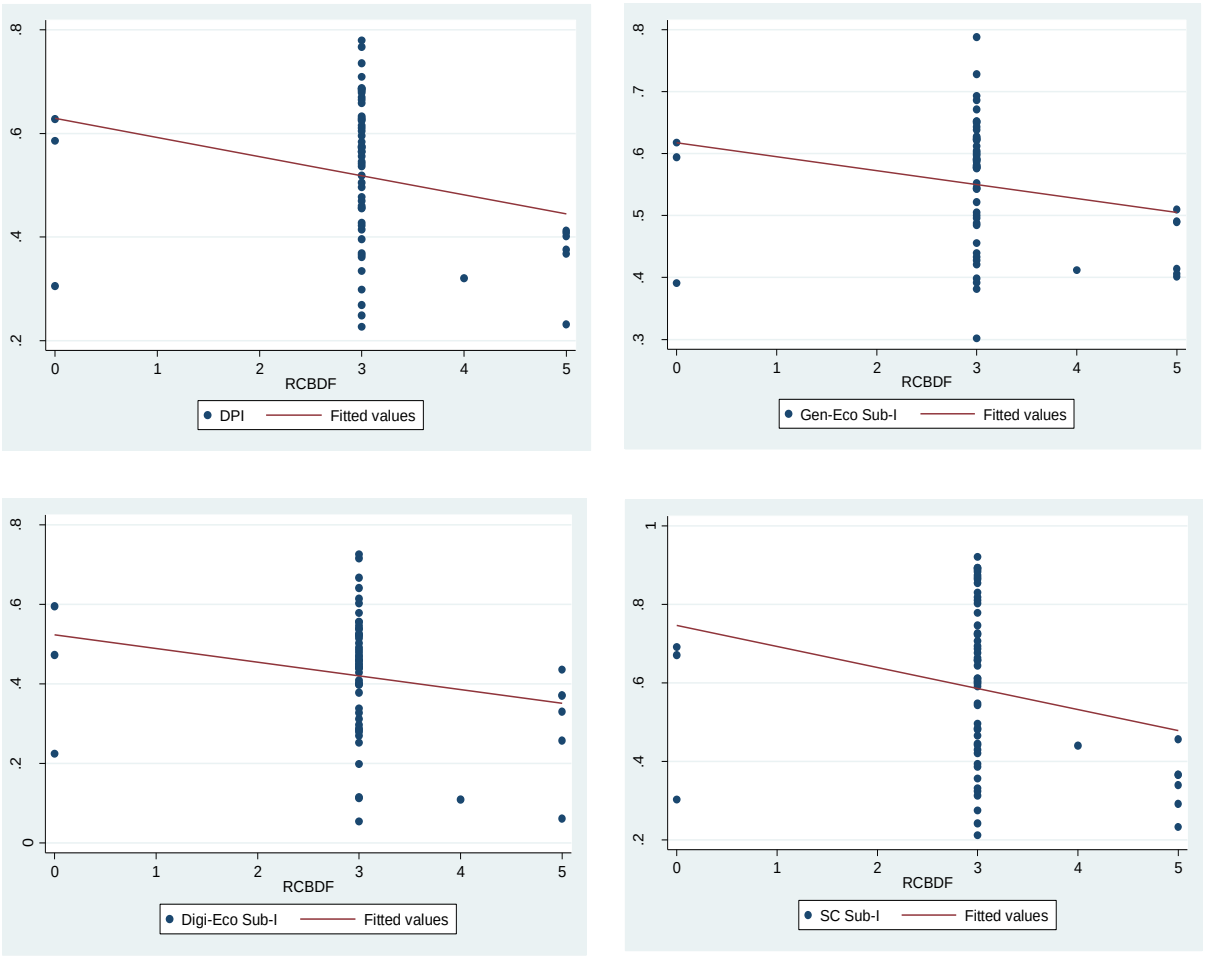
50 https://www.twobirds.com/en/news/articles/2020/global/pakistan-releases-updated-draft-of-personal-data-protection-bill

51 Please refer to Appendix 2 for country-wise RCBDF scores

52 We have also used Spearman's rank correlation, considering that the General RCBDF score can be considered an ordinal variable. The results from both correlation estimates do not vary by a significant degree.

53 Please refer to Appendix 2 for the correlation tables.

Figure 3.2: Correlations between the Digital Potential Index/ Sub-Indices and Data Localisation for Countries with Scores from 0 to 5

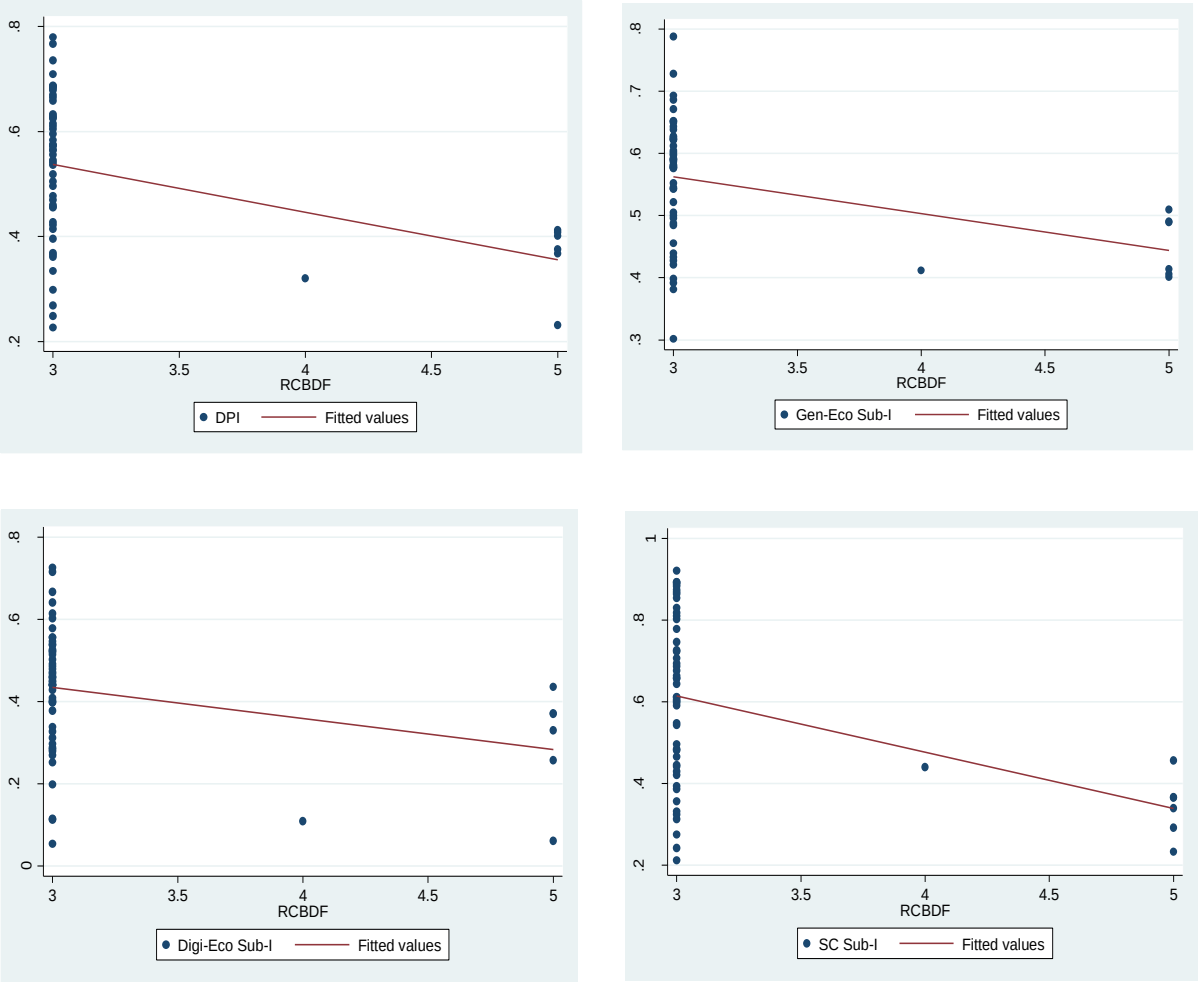


Source: Authors' calculations

Next, we do the same exercise for only those countries *do not* have unconditional cross-border data flows (scores ranging from 3 to 5), and run similar correlations. Correlation estimates for both Pearson's correlation and Spearman's rank correlation are negative. While the correlation values are not very high, they are all statistically significant. Figure 3.3 provides a graphical representation of Pearson's correlation estimates.[54] Overall, the correlation results show that restrictions imposed on cross-border data transfers are likely to be less stringent if a country has a stronger general economy sub-index and/ or state capacity sub-index. The direction of the result is similar for the digital economy sub-index but surprisingly, its strength is weaker.

[54] Please refer to Appendix 2 for the correlation tables.

Figure 3.3: Correlations between Digital Potential Index/ Sub-Indices and Data Localisation for Countries with Data Localisation Measures



Source: Authors' calculations

On the whole, the correlations show that the higher a country ranks on the Digital Potential Index, i.e., the more developed the country is in terms of its general economy, digital economy and higher its state capacity, the less stringent its restrictions on cross-border data flows are likely to be. It is noteworthy here that a majority of countries in our sample have a General RCBDF score of 3, with the combination of *conditional flow without local storage requirements, personal data and active* (based on the afore-mentioned scoring parameters). For example, most EU countries under the GDPR have this score. Coincidentally, most of them also rank relatively highly on the DPI as well as the sub-indices.

Arguably, the GDPR is on its way to becoming the gold standard for data protection laws around the world. Perhaps, countries that are performing well on most fronts and have strong state capacity could potentially draw from the GDPR's emphasis on individual rights and explicit consent, and a system based on data protection adequacy requirements can soon become the global norm. For example, Singapore, which ranks first on the DPI has strict

adequacy requirements for cross-border data transfers, but with the overarching guiding principle of open and transparent flow of data across borders with adequate protection standards.[55] Singapore is also part of the Cross-Border Privacy Rules (CBPR) and Privacy Recognition for Processors (PRP) systems, thus ensuring high standards of protection for personal data, without imposing localisation or other stringent requirements.[56] Other countries that are part of these multi-lateral systems include USA, Mexico, Canada, Japan and Korea.[57] Except for Mexico, all the other countries rank within the top 20 countries on the DPI. Mexico, although with a comparatively lower DPI rank, still ranks much above India. In an increasingly data-intensive and interconnected global economy, unfettered data flows, albeit ideal, might not be completely realistic. Therefore, bilateral and pluri-lateral agreements might pave the way to ensure transparent data flows with adequate protection in place.

The case of Luxembourg with the second rank on the DPI also supports our results. In the European Commission's 'Digital Economy & Society Index (DESI)', 2019, it ranks 6th among the European Union countries.[58][59] Much of this is attributed to the country's 'open data policy' which provides for the possibility of universal access to public data, thereby enabling individuals, businesses and the media to reuse, combine or share data for any appropriate purpose, including commercial ones.[60] An open data policy not only makes public-sector activities more transparent; it also encourages public actors to make better use of their resources.[61] Not surprisingly, Luxembourg ranks highly on the state capacity sub-index and scores a 3 on General RCBDF measures owing to its compliance with GDPR.

While the general result of our analysis is valid and intuitive, there are exceptions. For instance, all the countries with the highest RCBDF score of 5, except for Pakistan, rank higher than India on the DPI as well as the general economy and digital economy sub-indices, despite India having a lower RCBDF score. On the state capacity sub-index, however, India ranks higher than all these countries, except for Indonesia. Moreover, the correlations between the DPI/ sub-indices with the Sectoral RCBDF scores are extremely weak and not statistically significant. This might indicate that the approach or the stringency of sectoral data regulations are not typically influenced or affected by the overall strength of an economy and its state capacity. However, the evidence to support such an inference is not robust. Moreover, most countries are still in a state of flux with respect to their sectoral data flow regulations, existing or potential overlaps between them and the overarching framework, as well the decision of whether data localisation or restricted flows fall within the ambit of sectoral regulators. For example, the data localisation requirements in the draft national e-commerce policy in India which was released in 2019, have now been diluted and the matter has been left to the discretion of the Ministry of Electronics and Information Technology to

55 https://practiceguides.chambers.com/practice-guides/data-protection-privacy-2020/singapore
56 Ibid
57 Ibid
58 https://luxembourg.public.lu/en/invest/competitiveness/desi.html
59 https://ec.europa.eu/digital-single-market/en/scoreboard/luxembourg
60 https://data.public.lu/en/strategy/
61 https://gouvernement.lu/en/dossiers/2018/open-data.html#bloub-3

be addressed in the PDP Bill.[62] Therefore, a purely quantitative/ empirical exercise leaves gaps in the overall understanding of data regulations. For a more in-depth and reflective understanding, we develop a few country examples to dissect the type and extent of localisation measures keeping in mind the country specific characteristics captured in the sub-indices developed above. The case studies naturally present a more nuanced picture of the entire data regulation landscape.

4. Case Studies

A deep-dive into specific data localisation measures by countries provides a more nuanced picture of the global data localisation landscape. In this section, we have conducted an in-depth review of four individual data localisation measures of Indonesia, Vietnam, Australia and South Korea which are available in Appendix 3. The key themes that emerge are:

- Motivation and scope
- Cost implications
- Enforcement challenges and consequences

Motivation and Scope

The scope of data localisation measures usually reflects the motivation behind it. A specific tailored data localisation measure usually has a narrow scope covering a specific type of data and related to only to a particular sector. The Edward Snowden episode of 2013 has been considered a key trigger towards many countries proposing data localisation as a solution to prevent surveillance in foreign jurisdictions. However, a closer examination of individual cases of data localisation measures reveals varied motivations stretching back to times before the Snowden revelations. The data localisation measures in Australia and South Korea are examples of regulations that mandated data localisation before concerns around surveillance in foreign jurisdictions emerged. Both countries have a very specific data localisation mandates restricted in scope. For example, in Australia, it is restricted to health data as provided under the My Health Record System (erstwhile Personally Controlled Health Records Act). In South Korea the data localisation measure is specifically targeted to spatial and location data. However, their overarching data protection laws allow for conditional cross-border flows of personal data without local storage requirements. These examples point to a very specific motivation behind the localisation requirement. Australia is motivated by its need to protect health data of its citizens and potential privacy concerns from an already contested health program, while South Korea is motivated by the need for tighter security measures on mapping and spatial data due to its long-standing security threats from the North. The more recent data localisation measures such as that in Indonesia, and Vietnam, have a broader scope. The motivations behind such broad measures are the protection of data privacy of citizens and easier access of data to law enforcement agencies within the country.

[62] https://www.livemint.com/politics/policy/data-storage-rules-out-of-e-commerce-policy-1561488393145.html

However, there are also allied motivations that are not explicit such as greater control of online dissent[63] or even the promotion of domestic industry[64].

Cost Implications

The most immediate response to data localisation measures is with regard to the costs involved. The cost implications involved at a country level can be understood in two ways: first, the cost of required infrastructure and enabling environment; and second, the compliance costs to entities affected by the localisation measures.

Data localisation measures are costly in terms of creating the infrastructural environment that enables data localisation, such as providing land, continuous power supply, cooling systems etc. for establishing and running a data center: estimates[65] suggest that a data center 'rack' costs approximately $120,000 in capital over its 10 year lifetime, with electricity (20%), engineering (18%), power and server equipment (18%), facility space (15%) and maintenance (15%) garnering top shares when costs are broken down. Vietnam[66] was ranked 90th in technology and innovation, and 70th in human capital, among 100 countries, rankings that reflect an absence of readiness for Industry 4.0. Moreover, a global cloud computing ranking finds Vietnam stagnating in its position (24th out of 24 countries) of preparedness for adoption and growth of cloud computing, signaling an environment not conducive for building data-centre infrastructure[67]. Along with Vietnam, Indonesia too lags behind and is ranked at 23rd out of 24 countries.[68] While the investments in data centre infrastructure continue to grow with internet companies investing heavily[69], Indonesia remains a highly earth-quake prone zone, and building resilient infrastructure would add additional costs as compared to other locations[70].

The cost of compliance to entities under the ambit of the data localisation measure is the other aspect to be considered. A study[71] that estimates costs of compliance (and non-compliance) with data protection regimes at country and state levels, with the GDPR as a benchmark case, finds that the average costs of compliance for an organization is $5.47 million, and varies by the industry sector ranging from $7.7 million for media to more than $30.9 million for financial services. Typical sources of costs in complying with data protection regulations involve incident response plans, compliance audits and assessments,

63 https://www.reuters.com/article/us-vietnam-socialmedia-exclusive/exclusive-vietnam-cyber-law-set-for-tough-enforcement-despite-google-facebook-pleas-idUSKCN1MK1HL

64 https://www.fticonsulting-asia.com/~/media/Files/apac-files/insights/articles/localisation-to-fragment-data-flows-asia.pdf

65 See: http://www.linuxlabs.com/PDF/Data%20Center%20Cost%20of%20Ownership.pdf and, https://www.datacenterknowledge.com/archives/2015/02/11/data-center-building-vs-outsourcing-whats-best-business

66 See: WEF, Readiness for the Future of Production Report (2018)

67 See: https://cloudscorecard.bsa.org/2018/pdf/BSA_2018_Global_Cloud_Scorecard.pdf

68 https://cloudscorecard.bsa.org/2018/pdf/country_reports/2018_Country_Report_Indonesia.pdf

69 https://asia.nikkei.com/Business/Business-Trends/Data-center-competition-heats-up-in-Southeast-Asia; https://www.datacenterdynamics.com/news/amazon-invest-951m-indonesia/

70 http://www.ciscopress.com/articles/article.asp?p=417091

71 See: http://dynamic.globalscape.com/files/Whitepaper-The-True-Cost-of-Compliance-with-Data-Protection-Regulations.pdf

redress activities among others. The responses of countries to cost implications have been different. Both Vietnam and Indonesia proceeded with their legislations, with Indonesia diluting the scope of data localisation requirements owing to concerns with the previous regulation.[72] Meanwhile, Vietnam too, is contemplating easing its localisation requirements amidst widespread criticism.[73]

Enforcement Challenges and Consequences

Data localisation legislations are historically novel and thus knowledge of relative success in enforcing such measures is limited. However, available country level experiences inform the challenges in enforcing data localisation legislations.

As explicated in the case studies[74], countries that introduced broad based data localisation requirements faced difficulties with compliance, followed by intense lobbying geared towards amending such requirements to more specific requirements. In cases where there was resistance to compliance, as in the case with Telegram in Russia[75] the state found it difficult to fully block access to the messaging app,[76] while incurring significant costs and efforts towards such attempts[77].

A source of challenge in enforcing data localisation legislations is the formulation of the categories of data. In cases of both Indonesia[78] and China[79], the initial legislation that mandated data localisation requirements were defined in ways that industry bodies in the respective countries found it ambiguous[80]. In the case of Indonesia, a 5-year period to meet data localisation requirements met with widespread non-compliance and lobbying that eventually triggered an amendment towards more specific data localisation requirements, whereas in China, companies have only started to become compliant[81], as the Government seeks to clear any remaining ambiguity[82]. Industry wide lobbying however compelled China to postpone legislating data localisation requirements until late into 2018.[83,84] This illustrates the costs of strict enforcement of data localisation requirements despite non-compliance.

Data localisation requirements that were shaped by unique circumstances, in the case of South Korea, have experienced strict enforcement: South Korea's data localisation[85], which was formulated as a wartime measure to prevent location data from being available to its neighboring enemy North Korea, witnessed success in terms of restricting location data

72 https://www.mondaq.com/data-protection/861082/government-relaxes-data-localisation-requirement
73 https://www.medianama.com/2019/10/223-data-localisation-vietnam/
74 See Appendix III
75 See: https://www.theverge.com/2018/4/17/17246150/telegram-russia-ban
76 See: https://www.wired.co.uk/article/telegram-in-russia-blocked-web-app-ban-facebook-twitter-google
77 See: https://www.nytimes.com/2018/04/18/world/europe/russia-telegram-shutdown.html
78 See: Appendix for Case study
79 See: https://jsis.washington.edu/news/chinese-data-localisation-law-comprehensive-ambiguous/
80 Ibid
81 See: http://www.xinhuanet.com//politics/2017-08/14/c_1121482148.htm
82 See: https://jsis.washington.edu/news/chinese-data-localisation-law-comprehensive-ambiguous/
83 See: https://www.nytimes.com/2017/05/31/business/china-cybersecurity-law.html
84 See: https://www.nytimes.com/2018/04/18/world/europe/russia-telegram-shutdown.html
85 See: Appendix for Case study

within its borders through localisation measures. Consequently, and over the years, data localisation requirements compelled foreign companies to negotiate with South Korea for access to location, while creating competitive indigenous location-based industries[86].

5. Conclusions and Policy Perspectives

Localisation norms in India already exist through different laws and policies, prior to the discussions in the Personal Data Protection Bill, 2019, as discussed previously in this report. The discussion on data localisation was re-ignited with the Draft Personal Data Protection bill, 2018.

The motivations for data localisation measures in India, as reviewed in the previous sections, broadly stem from privacy, security and protectionist ends. RBI's data localisation directive cited security and monitoring as a key motivation, whereas, erstwhile data localisation requirements within the draft National Policy Framework for E-Commerce in India was viewed as a protectionist measure being egged on by domestic companies including data centers and digital payments groups.[87]

India is at a crucial juncture with respect to its policies on data regulation. It presents a timely opportunity to examine the implications of data localisation measures, and potential impact it will have on the economic fabric in India.

This study surveyed various restrictions to cross-border data flows being implemented in varying degrees across different countries. What is central to widespread deliberations and legislations on such restrictions is the acknowledgement of the value of data flows and its significance to national economies. Associated with this knowledge is also the view that the lack of adequate protection for data flows pose a threat to national sovereignty. This view considered to have stemmed from the Edward Snowden disclosures inspired national governments to propose data localisation measures to ensure cyber-security and privacy of individuals within the country.

Although data has been widely acknowledged to create economic value, its valuation has proven elusive as yet. As a result, economic impacts of data localisation measures, both at the micro and macro level are yet to be fully understood. This is due to the fact that many countries are at the stage of legislating, amending, or enforcing data protection measures, in general and data localisation measures, if any, in particular. In theory, stronger restrictions placed on data implies that it could harm innovation and competition in an economy and thereby erode the value derived from data. For example, bigger entities have the means to comply with data localisation measures, meaning it also allows them to control data more firmly. At the same time, there may be a trade-off between data markets and privacy. In the absence of explicit valuation models, this study presents case studies that reviews various data regulation and localisation measures, the reaction in countries, and the implication and challenges that follow from such measures. Besides, the inference from international

[86] Ibid
[87] https://www.ft.com/content/92bb34a8-b4e5-11e8-bbc3-ccd7de085ffe

comparisons based on derived indices shows that strength of a country's macroeconomic climate, digital economy and state capacity allows for a more robust and permissive regime with respect to cross-border data flows.

This broad result offers a yardstick with which to compare specific country experience that we build in the case studies presented in the appendix. For example, does the country experience agree with and indeed reinforce our finding or does it run contrary to our overall result. In other words, what are some of the other considerations that inform the utility of data localisation measures beyond those used in construction of the index. Besides, the following characteristics are worth emphasizing.

1. *Regulatory Impact Assessment*: There has not been any clear evidence on the possible effects of data localisation, in terms of improving security, or promoting the domestic economy. However, at the enterprise/entity/firm level, there is evidence of opposition due to data localisation's uncertain impacts on cost structures, and the strain on firm-level capabilities to comply. A regulatory impact assessment along with broad based stakeholder consultations will better inform policy on the risks associated with data localisation.
2. *Specificity of data localisation:* As highlighted in the case studies section, data localisation measures that are broad in scope as in the case of Indonesia and Vietnam have experienced challenges with feasibility. Data localisation measures that are engineered for specific purposes have experienced success where strict enforcement complemented by quality institutions was available as in the case of South Korea. Strict enforcement was not possible, as in the case of Australia, as the purpose for which data localisation requirements were mandated experienced a crisis of credibility. But more fundamentally, specificity of data localisation points towards the capabilities to enforce such requirements, measured by state capacity, and the relative costs of uncertainty on the economy caused by data localisation measures. China amended broad ranging data localisation in favor of more specific recommendations, in response to industry lobbies expressing concerns over uncertainty in compliance costs and regulatory uncertainty.
3. *Co-ordinated strategies towards Data localisation measures*: Currently, there is evidence of absence of co-ordination among regulatory authorities in defining the contours of data protection[88]: there were simultaneous, un-coordinated consultations on data protection conducted by the Srikrishna Committee and the TRAI. In 2018, the RBI mandated payment systems data to be localized before any legislation on data protection, which amidst criticism from the industry is currently under review. This is set to create regulatory uncertainty. As the Srikrishna committee itself stated that sectoral regulators are set to play a key role in taking India's data protection forward, greater coordination among various sectoral regulators will be significant towards a harmonized data protection regime.

[88] See: https://inc42.com/resources/what-will-be-the-fate-of-trai-recommendations-and-the-rbi-circular-after-the-pdp-bill-is-enacted/

4. *Requisite regulatory environment:* While a case can be made for data localisation to serve legitimate purposes of privacy and security, a localisation mandate must be contextualized in the broader institutional environment addressing privacy and security requirements of the country. As can be learnt from Australia's case study, data localisation requirements provide no additional confidence in privacy and security measures, if the design of complementary institutions and mechanisms (such as the My Health Records system) do not enjoy credibility or legitimacy.
5. *Fixing liability and burden of Costs*: The alleged underlying motivation of data localisation measures is that data protection provided by the State that mandates such requirements is at least as good as the next best alternative, i.e. data protection by data processors. What data localisation does is make the State at least in part liable for data protection, shifting the burden of providing the enabling environment and infrastructure for data in part on to the State.

Data localisation risks misaligning incentives[89] and consequently risks privacy and security it seeks to improve: since data processors derive and maximize value from data generated by customers, and thus consequently value holding on to customers from whom such data is derived from, data localisation, by shifting liability at least in part to the State, which does not directly derive value from, thus risks misaligning incentives, leading to inefficient outcomes.

[89] See Anderson and Moore (2006)

Bibliography

'The Global Risks Report 2020', *World Economic Forum*

'The Localisation Gambit'. The Centre for Internet and Society (2019)

'The State of the Network 2020 Edition', *Telegeography*

Aaronson, S.A. "The Digital Trade Imbalance and Its Implications for Internet Governance". Center for International Governance Innovation and Chatham House (2016).

Acemoglu, D., Garcia-Jimeno, C., Robinson, J.A. "State Capacity and Economic Development: A Network Approach: Dataset", *American Economic Review*, 105(8), (2015): 2364-2409.

Acemoglu, D., Moscona, J., Robinson, J.A. "State Capacity and American Technology: Evidence from Nineteenth Century". *American Economic Review* 106, no.5 (2016): 61-67

Acemoglu, D., Robinson, J.A. "Why Nations Fail: The Origins of Power, Prosperity, and Poverty" *Finance and Develpoment- English Edition*, 49, no. 1 (2012)

Amsden, A.H. "Asia's Next Giant: South Korea and Late Industrialization". New York: Oxford University Press (1989).

Anderson, R., Moore, T. "The Economics of Information Security". *Science*, New Series, Vol. 314, No. 5799 (October, 2006): 610-613

Bailey, R., Bhandari, V., Parsheera, S., Rahman, F. "Comments on the (Draft) Personal Data Protection Bill, 2018", National Institute of Public Finance and Policy, New Delhi.

Bailey, R., Parsheera, S, "Data Localisation in India: Questioninf the means and ends". National Institute of Public Finance and Policy, New Delhi.

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

Bauer, M., Lee-Makiyama, H., van der Marel, E., Verschelde, B. "The Costs of Data Localisation: Friendly Fire on Economic Recovery", *ECIPE Occasional Paper*, No.3 (2014)

Besley, T., Persson, T. "The Origins of State Capacity: Property rights, taxation, and politics". *American Economic Review* 99, no. 4 (2009): 1218-44

Calhoun, C.J. (Ed.). "Dictionary of Social sciences". New York: Oxford University Press (2002).

Castro, D., Mcquinn, A. "Cross-Border Data Flows Enable Growth in All Industries" *Information Technology and Innovation Foundation* (2015)

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

Centeno, M.A. "Blood and Debt: War and Nation State in Latin America". Princeton: Princeton University Press (2002).

Chander, A., Le, U.P. "Data Nationalism". *Emory Law Journal*, 64 (2014): 677-739

Chibber, V. "Building a Developmental State: The Korean Case Reconsidered", *Politics and Society*, Vol. 27 No. 3 (September, 1999): 309-346

Corey, Nigel. "Cross-Border Data Flows: Where are the barriers, and what do they cost? "*Information Technology & Innovation Foundation* (2017)

Dinecco, M. "State Capacity and Economic Development: Present and Past". Cambridge University Press (2017).

Enriquez, E., Centeno, M.A. "State Capacity: Utilization, durability, and the role of wealth vs. History". *International and Multidisciplinary Journal of Social Science*, 1, no. 2 (2012): 130-162

Evans, P. "Embedded Autonomy: States and Industrial Transformation". Princeton: Princeton University Press (1995).

Ferracane, M.F. "Restrictions on Cross-Border data flows: a taxonomy" *ECIPE Working Paper* No. 1 (2017).

Herbst, J. "States and Power in Africa: Comparative Lessons in Authority and Control". Princeton: Princeton University Press (2000).

Hinman, L. "Esse est indicator in google" Ethical and political issues in search engine". *International Review of Information Ethics,* 3(6), (2005): 19-25

Internet and Mobile Association of India (IAMAI). "Internet in India 2016". Strategic Research (2017)

Johnson, C.A. "MITI and the Japanese Miracle: The Growth of Industrial Policy, 1925-1975". Stanford: Stanford University Press (1982)

Johnson, D.R., Post, D. "Law and Borders: The rise of law in cyberspace" *Stanford Law review* (1996): 1367-1402

Johnson, N.D., Koyama, M. "States and Economic Growth: Capacity and Constraints: *Explorations in Economic History* 64 (2017): 1-20

Kathuria, Rajat, Mansi Kedia, Gangesh Varma, and Kaushambi Bagchi. "Economic Implications of Cross-Border Data Flows." *ICRIER* (2019).

Knutsen, C.H. "Democracy, State Capacity, and Economic Growth". *World Development* 43 (2013): 1-18

Kuner, C. "Regulation of Trans border Data Flows under Data Protection and Privacy Law: Past, Present and Future", Netherlands, Tilburg University (2011): 5-6

Laidlaw, E. "Private power, public interest: An examination of search engine accountability". *Internet Journal of Law and Information Technology,* 17(1), (2008): 113-145

Manyika, J., Lund, S., Bughin, J., Woetzel, J., Stamenov, K., Dhingra, D. "Digital Globalization: The New Era of Global Flows". McKinsey Global Institute (MGI) (2016).

Michael, M. "The autonomous power of the state: its origins, mechanisms, and results". *European Journal of Sociology/Archives européennes de sociologie* 25, no.2 (1984): 185-213

Selby, J. "Data Localisation laws: Trade barriers or legitimate responses to cyber security risks, or both?" *International Journal of Law and Information Technology* 25, no. 3 (2017): 213-232.

Shapiro, A.L. "The Control Revolution: How the Internet is putting individuals in charge and changing the world we know". New York: Public Affairs (2000)

Taddeo, Mariarosaria., Floridi, Luciano. "The debate on the moral responsibilities of online service providers". *Science and Engineering Ethics,* 22, no.6 (2016): 1575-1603

Timothy, B., Persson, T. "Pillars of Prosperity: The Political Economics of Development Clusters". Princeton University Press (2011).

U.S. Chamber of Commerce., Hunton & Williams. "Business Without Borders: The Importance of Cross-Border Data Transfers to Global Prosperity" (2014)

United Nations Conference for Trade and Development. "Data protection regulations and international data flows: Implications for trade and development". United Nations Publications (2016).

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

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

Wade, R.H. "Governing the Market". Princeton: Princeton University Press (1990)

Appendix

Appendix 1

Country	DL Measure	Scope of Data Types	Scope of Sectors Affected	Status
Argentina	Section 12 of the Data Protection Act of Argentina (Law 25,326) prohibits the transfer of personal data to countries that do not have an adequate level of protection in place, but such countries have not been identified yet. The Regulatory Decree No. 1558/2001 provides that the prohibition is not applicable when the data subject has expressly consented to the transfer. Data can also be transferred to a foreign country by means of an international agreement between the data controller and the foreign processor, under which the latter undertakes to comply with the same standards of protection and other legal obligations as provided in the Argentine data protection regulations.A bill has been recently presented to Congress that would replace Law 25326 in order to align data protection standards with the GDPR.[118] Resolution 04/2019 aims 'to unify the criteria of the Agency of Access to Public Information for the correct interpretation and implementation of the current regulations on the protection of personal data, whose observance is mandatory.	Personal Data	Across all sectors	Active
Australia	1. The Personally Controlled Electronic Health Record Act of 2012 requires local data centres to handle 'personally controlled electronic health records'. Therefore, no electronic health information can be held or processed outside Australia, unless they do not "include information in relation to a consumer"or they are "identifying information of an individual or entity". An Amendment passed in 2018 "removed the ability of the My Health Record System operator to disclose health information in My Health Records to law enforcement and government agencies without an order by a judicial officer or the healthcare recipient's consent; and require the system operator to permanently delete from the National Repositories Service any health information about a healthcare recipient who has cancelled their My Health Record.	Health Data	Specific Sector	Active
	2. Under the Federal Privacy Act, before an organization discloses personal information to an overseas recipient, it must take reasonable steps to ensure that the overseas recipient will not breach the Australian Privacy Principles (APPs). This requirement does not apply only if: - the overseas recipient is bound by a law similar to the APPs that the data subject can enforce; - the data subject consents to the disclosure of the personal data in the particular manner prescribed by APP; or - another exception applies. An organisation may be held liable for any breaches of the APPs by that overseas recipient.	Personal Data	Across all sectors	Active. The law is in force, however, data need not be localised under specific conditions.
Belgium	1. Article 463 of the Companies Code requires that the company register of shareholders and register of bonds must be kept at the registered office of the company. Since 2005, it is possible to keep the registers in electronic format as long as they are accessible at the registered office of the company	Company Records	Across all sectors	Active. The law is in force, however, data need not be localised under specific

Country	DL Measure	Scope of Data Types	Scope of Sectors Affected	Status
				conditions.
	2. With respect to VAT, invoices received and copies of invoices issued by the taxpayer must be stored in Belgium or in another EU member state under certain conditions. Invoices must be stored either in electronic or paper format (Article 60, § 3 of the VAT Code).	Tax Data	Across all sectors	Active.
	3. With respect to income tax, other than in cases of exception granted by the administration, the books and documents must be kept at the disposal of the tax administration in the office, agency, branch or other professional or private premises of the taxpayer where they have been kept, prepared or sent. There are no data localisation requirements under Belgian law. Any data localisation requirements that existed in EU Member State law have been lifted following the entry into force of the GDPR, as well as EU Regulation 2018/1807 of 28 November 2018 on the free flow of non-personal data. Belgian data protection law supports all data-transfer mechanisms provided in the GDPR, including the use of standard contractual clauses, binding corporate rules, and the EU-U.S. Privacy Shield and accepts that data may be transferred on the basis of a derogation such as the individual's explicit consent. In principle, the individual concerned must be informed of the data transfer prior to the actual transfer, but the Belgian DP Act provides for exceptions in the area of law enforcement and intelligence services.	Tax Data	Across all sectors	Active. The law is in force, however, data need not be localised under specific conditions.
Brazil	In September 2013, Brazil began considering a policy that would have forced Internet-based companies, such as Google and Facebook, to store data relating to Brazilians in local data centers. It withdrew this provision from the final copy of the bill. Furthermore, in 2016, Brazilian government agencies, including the Secretary of Information Technology of the Ministry of Planning, Development, and Management, have included forced data localisation as a requirement for public procurement contracts involving cloud-computing services. August 14, 2018, Brazil approved the General Data Protection Law which will come into effect after its 18th adaptation period, in August 2020. The LGPD creates a new legal framework for the use of personal data in Brazil, both online and offline, in the private and public sectors. Currently, Brazilian law does not provide any restrictions specific to international data transfers but once the LGPD starts to be applied it will only be possible (Article 33): -to countries or international organisations that provide adequate levels of data protection; - when the controller offers and proves compliance with the principles and rights of the data subject and the regime of data protection, upon specific contractual clauses, standard contractual clauses, global corporate rules or regularly issued stamps; - when the transfer is necessary for international legal co-operation between public intelligence, investigative and prosecutorial agencies; - when the transfer is necessary to protect the life or physical safety of the data subject or of a third party; - when the ANPD authorises the transfer;	Personal Data and Public Procurements	Across all sectors	Active

Country	DL Measure	Scope of Data Types	Scope of Sectors Affected	Status
	- when the transfer results in a commitment undertaken through international cooperation; - when the transfer is necessary for the execution of a public policy or legal attribution of public service; - when the data subject has given his or her specific consent for the transfer, with prior information about the international nature of the operation, with this being clearly distinct from other purposes; and - when it is necessary to satisfy compliance with regulatory obligations by the controller, execution of a contract or preliminary procedures related to it and the regular exercise of rights in judicial, administrative or arbitration procedures.			
Bulgaria	Any data localisation requirements that existed in EU Member State law have been lifted following the entry into force of the GDPR, as well as EU Regulation 2018/1807 of 28 November 2018 on the free flow of non-personal data. In view of the entry into force of Regulation (EU) 2016/679 (General Data Protection Regulation - 'GDPR'), on April 30, 2018 a draft law amending and supplementing the Personal Data Protection Act ('Draft Law') was introduced for public discussion. Public consultations ended on May 30, 2018 and the Draft Law was submitted to the Parliament where it is subject to further amendments. The Draft Law designates the Commission for Personal Data Protection as the sole supervisor responsible for protecting the fundamental rights and freedoms of individuals with regard to the processing and free movement of personal data within the European Union. The Draft Law further regulates the legal remedies in cases of violation of personal data law, the accreditation and certification in the field of personal data protection, the administrative liability and the administrative measures in cases of violations of the Draft Law. It entered into force on 2 March, 2019. In Bulgaria, an applicant for a gaming license must ensure that all data related to operations in Bulgaria is stored on a server located in the territory of Bulgaria. Moreover, the applicant has to ensure that the communication equipment and the central computer system of the organiser are located within the EEA or in Switzerland.	Gaming Data	Specific Sector	Active
Canada	1. Nova Scotia requires that personal information held by a public body (primary and secondary school, universities, hospitals, government-owned utilities and public agencies) must be stored or accessed in Canada only. A public body may override the rules where storage or access outside of the respective province is essential. Moreover, the data can be transferred outside Canada "where the individual the information is about has identified the information and has consented, in the manner prescribed by the regulations, to it being stored in or accessed from, as the case may be, outside Canada".	Personal Data held by Public Body	Across all sectors	Active. The law is in force, however, data need not be localised under specific conditions.
	2. British Columbia requires that personal information held by a public body (primary and secondary school, universities, hospitals, government-owned utilities and public agencies) must be stored or accessed in Canada only. A public body may override the rules where storage or access outside of the respective province is essential. Moreover, the data can be transferred outside Canada "if the individual the information is about has identified the	Personal Data held by Public Body	Across all sectors	Active. The law is in force, however, data need not be localised under specific conditions.

Country	DL Measure	Scope of Data Types	Scope of Sectors Affected	Status
	information and has consented, in the prescribed manner, to it being stored in or accessed from, as applicable, another jurisdiction".			
	3. According to the Canadian Federal Law Personal Information Protection and Electronic Documents Act, consent is not necessary for the transfer of data to a third country as the Canadian law does not distinguish between domestic and international transfers of data. The company should, however, grant a comparable level of protection while the information is being processed by a third party. This is, preferably, achieved on a contractual basis with the third party.	Personal Data	Across all sectors	No Data Localisation mandated, however comparabale level of protection to be provided in foregin jursdiction
	4. In 2006, Québec amended its Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information to require public bodies to ensure that information receives protection "equivalent" to that afforded under provincial law before "releasing personal information outside Québec or entrusting a person or a body outside Québec with the task of holding, using or releasing such information on its behalf"	Personal Data	Across all sectors	No Data Localisation mandated, however comparabale level of protection to be provided in foregin jursdiction
China	1. The "Notice to Urge Banking Financial Institutions to Protect Personal Financial Information" states that the processing of personal information collected by commercial banks must be stored, handled and analysed within the territory of China, and such personal information is not allowed to be transferred overseas.	Financial Data	Specific Sector	Active. The implementing rules (18 May 2011) that clarify that PRC branches of foreign banks may transfer client information to their overseas headquarters, parent bank and subsidiaries for storage, processing and analysis if certain criteria are satisfied.
	2. Population health information needs to be stored and processed within China. In addition, storage is not allowed overseas.	Health Data	Specific Sector	Active.
	3. The transfer of data containing state secrets abroad is prohibited.	Data containing State Secrets	Across all sectors	Active
	4. China instituted a licensing system for online taxi companies which requires them to host user data on Chinese servers.	Multiple data types	Specific Sector	Active
	5. China has data residency laws that declare companies can store the data they collect only on	Multiple data	Across all	Active

Country	DL Measure	Scope of Data Types	Scope of Sectors Affected	Status
	servers in country	types	sectors	
	6. Online maps are required to set up their server inside the country and must acquire an official certificate.	Location and Map Data	Specific Sector	Active
	7. Strict guidelines for what can be published online and how the publisher should conduct business in China came into force in March 2016. According to the rules, any publisher of online content, including "texts, pictures, maps, games, animations, audios, and videos" will be required to store their "necessary technical equipment, related servers and storage devices" in China	Multiple data types	Across all sectors	Active
	8. The Cybersecurity Law includes requirements for personal information of Chinese citizens and "important data" collected by "key information infrastructure operators" (KIIOs) to be kept within the borders of China. If there are business needs for the KIIOs to transfer this data outside of China, security assessments must be conducted. The definition of KIIOs remains to be finalised. On May 28, 2019, the Cyberspace Administration of China ("CAC") released draft Data Security Administrative Measures (the "Measures") for public comment. The Measures, which, when finalized, will be legally binding, supplement the Cybersecurity Law of China (the "Cybersecurity Law") that took force on June 1, 2017, with detailed and practical requirements for network operators who collect, store, transmit, process and use data within Chinese territory. The Measures likely will significantly impact network operators' compliance programs in China.	Personal Data	Across all sectors	Active. The law is in force, however, data need not be localised under specific conditions.
	9. Article 5.4.5. of the Guidelines for Personal Information Protection Within Public and Commercial Services Information Systems prohibit the transfer of personal data abroad without express consent of the data subject, government permission or explicit regulatory approval "absent express consent of the subject of the personal information, or explicit legal or regulatory permission, or absent the consent of the competent authorities". If these conditions are not fulfilled, "the administrator of personal information shall not transfer the personal information to any overseas receiver of personal information, including any individuals located overseas or any organizations and institutions registered overseas". Although the Guidelines are a voluntary technical document, they might serve as a regulatory basis for judicial authorities and lawmakers. The Personal Information Security Specification, which came into force in May 2018, also stresses that explicit consent is required when sensitive data is being collected. The Specification is not a legally binding text, but the Chinese government agencies are likely to refer to it as a standard to determine whether companies are following China's data protection rules.	Personal Data	Across all sectors	Active. However, the guidelines are voluntary.
Colombia	Pursuant to Law 1266 of 2008, personal data may not be transferred outside of Colombia to countries which do not comply with the adequate standards of data protection. This restriction does not apply in the following cases: - when there is an express authorisation by the data	Personal Data	Across all sectors	Active. The law is in force, however, data need not be localised

Country	DL Measure	Scope of Data Types	Scope of Sectors Affected	Status
	subject; - when the information relates to medical data as required by issues of health and public hygiene; - for banking operations; and - for operations carried out in the context of international conventions which Colombia has ratified. "Statutory Law 1581 of 2012 (Law 1581) regulates personal data processing, as well as databases. Law 1581 is applicable to all data collection and processing in Colombia, except data regulated under Law 1266 and certain other types of data or regulated industries. Decree 1377 of 2013 (Decree 1377), is a piece of secondary regulation related to Law 1581 which outlines requirements for personal and domestic databases regarding authorization of personal data usage and recollection, limitations to data processing, cross-border transfer of data bases and privacy warnings, among others. This Decree also requires that controllers and processors to adopt a privacy policy and privacy notice." Decree 886 of 2014 (Decree 886) and Decree 090 of 2018 (Decree 090) issued by the Ministry of Commerce, Industry and Tourism as well as the Resolution 090 of 2018 issued by the Superintendence of Industry and Commerce, regulate the National Register of Data Bases and sets deadlines for registration of existing databases in Colombia. [90]			under specific conditions.
Cyprus	Cyprus has failed to replace several restrictive provisions under the Directive on Data Retention, which was declared invalid by the Court of Justice of the European Union (ECJ). This directive required data operators to retain certain categories of traffic and location data (excluding the content of those communications) for a period between six months and two years and to make them available, on request, to law-enforcement authorities for the purposes of investigating, detecting, and prosecuting serious crime and terrorism. Any data localisation requirements that existed in EU Member State law have been lifted following the entry into force of the GDPR, as well as EU Regulation 2018/1807 of 28 November 2018 on the free flow of non-personal data. The Protection of Physical Persons Against the Processing of Personal Data and Free Movement of such Data Law 125(I)/2018, that implements certain provisions of the GDPR into local law, entered into force on July 31, 2018 (the "Law").			
Denmark	1. The basis of the Bookkeeping Act (section 12) is that financial records must be stored in Denmark or in the Nordic countries. This applies to both physical appendixes and digital data. Hence, if financial records are stored on a server physically placed outside Denmark a complete copy must be kept in Denmark.	Company Records (Financial)	Across all sectors	Active.
	2. The basis for the Audit Act (section 45) is that financial records for governmental institutions must be stored in Denmark. This applies to both physical appendixes and digital data. This regulation means that financial records may be stored on a server abroad provided that an exact copy of the records is made on a monthly basis at a minimum. Such copy must be placed on a server in Denmark or in paper.	Government Data (Financial)	Specific Sector	Active

90 Law in Colombia - DLA Piper Global Data Protection Laws of the World

Country	DL Measure	Scope of Data Types	Scope of Sectors Affected	Status
	The new Danish Data Protection Act has come into force along with the GDPR on May 25, 2018 and repeals the Danish Personal Data Processing Act. Any data localisation requirements that existed in EU Member State law have been lifted following the entry into force of the GDPR, as well as EU Regulation 2018/1807 of 28 November 2018 on the free flow of non-personal data. To implement the GDPR, the Danish Parliament enacted the Danish Act on Data Protection (the 'Danish Data Protection Act') on May 17, 2018, enforceable on May 25, 2018 and replacing the previous Danish Act on Processing of Personal Data (Act no. 429 of 31/05/2000). Hence, data protection and processing in Denmark is now regulated by the GDPR as supplemented by the Danish Data Protection Act. The Danish Data Protection Act does not apply to Greenland and the Faroe Islands.	Personal Data	Across all sectors	Active.
European Union	The European Union has updated its data protection regime by replacing the Directive 95/46/ EC with the General Data Protection Regulation (GDPR). The Regulation was approved in April 2016 and it has been in force with immediate effect on all 28 EU Member States from 25 May 2018. Formally adopted on 14 November 2018 by the European Parliament and the Council's, the Regulation (EU) 2018/1807 is a framework for the free flow of non-personal data in the European Union. It is the follow-up to GDPR and is another major pillar in the EU's drive to create a Digital Single Market. Non-personal data' is defined as any data that doesn't constitute personal data under Article 4 of GDPR. The prominent change being introduced by Regulation (EU) 2018/1807 is that member states will be prohibited from enforcing data localisation in relation to the processing or storing of non-personal data. The aim of this is to promote the free movement of non-personal data across the EU without any interference from member states. The only exemption from this prohibition comes in the form of restrictions on movement when necessary for public security. In order to avail of this exemption, the relevant member state must communicate any remaining or proposed data localisation policies to the European Commission along with their justifications for the restriction.	Personal Data	Across all sectors	Active. The law is in force, however, data need not be localised under specific conditions.
Finland	The Accounting Act requires that a copy of the accounting records in kept within Finland. Alternatively, the records can be stored in another EU country if a real-time connection to the data is guaranteed. Any data localisation requirements that existed in EU Member State law have been lifted following the entry into force of the GDPR, as well as EU Regulation 2018/1807 of 28 November 2018 on the free flow of non-personal data. Finland has passed a supplementary implementation act of the GDPR, the Data Protection Act of Finland (Tietosuojalaki), which repeals the Personal Data Act (523/1999), as well as the Law on the Data Protection Board and the Data Protection Commissioner (389/1994). The Data	Company Records	Across all sectors	Active

Country	DL Measure	Scope of Data Types	Scope of Sectors Affected	Status
	Protection Act of Finland entered into force on 1 January, 2019.			
France	A ministerial circular dated 5 April 2016 on public procurement states that it is illegal to use a non- "sovereign" cloud for data produced by public (national and local) administration: all data from public administrations have to be considered as archives and therefore stored and processed in France. Any data localisation requirements that existed in EU Member State law have been lifted following the entry into force of the GDPR, as well as EU Regulation 2018/1807 of 28 November 2018 on the free flow of non-personal data. France adapted its domestic legislation to GDPR with the enactment of (i) Law No.2018-493 of June 20, 2018 on the protection of personal data, which mainly updates Law No. 78-17 of January 6, 1978 on information technology, data files and civil liberties, the principal law regulating data protection in France (the "Law") and (ii) Decree No. 2018-687 of 1 August 2018 implementing the Law, which updates the Decree No. 2005-1309 of 20 October 2005 (the "Decree"). In addition, the Order No. 2018 of December 12, 2018, adopted pursuant to Article 32 of Law No. 2018-493, updates the Law and other French laws relating to personal data protection in order to "*simplify the implementation and make the necessary formal corrections to ensure consistency with EU data protection law*" (the "Order"). The Order will enter into force on June 1, 2019. The Decree will be amended before June 1, 2019 by another decree, in order to take into account the revisions introduced by the Order. In addition, French rules adopted on the basis of the leeway left to Member States by the GDPR will apply only to the extent the data subject resides in France, including when the data controller is not established in France, with an exception for processing carried out for journalistic purposes or the purpose of academic, artistic or literary expression. For such processing activities, the national rules of the Member State where the data controller is established apply, to the extent such controller is established in the European Union.	Multiple data types	Across all sectors	Active. The law is in force, however, data need not be localised under specific conditions.
Germany	1. The Act on Value Added Tax states that invoices must be stored within the country, including when stored electronically. Alternatively, in case of electric storage, they may be stored within the territory of the EU if full online access and the possibility of download are guaranteed. In this case, the entity is obliged to notify the competent tax authority in writing of the location of the electronically stored invoices, and the tax authority may access and download the data	Tax Data	Across all sectors	Active.
	2. Under the Tax Code, all persons and companies liable to pay taxes that are obliged to keep books and records must keep those records in Germany. There are some exceptions for multinational companies.	Tax Data	Across all sectors	Active
	3. According to the German Commercial Code, accounting documents and business letters must be stored in Germany.	Company Records	Across all sectors	Active
	4. Under the Directive on Data Retention, operators were required to retain certain categories of traffic and location data (excluding the content of those communications) for a period of	Telecommunications Data	Specific Sector	Active

Country	DL Measure	Scope of Data Types	Scope of Sectors Affected	Status
	between six months and two years and to make them available, on request, to law enforcement authorities for the purposes of investigating, detecting and prosecuting serious crime and terrorism. On 8 April 2014, the Court of Justice of the European Union declared the Directive invalid. However, not all national laws which implemented the Directive have been overturned. In 2010, the German Constitutional court found the implementation of the Directive on Data retention to be unconstitutional. Yet, in October 2015, a new data retention law was passed, which will enter into force in 2017. The law provides that telecommunication providers must retain data such as phone numbers, the time and place of communication (except for emails), and the IP addresses for either four or 10 weeks. The data is to be stored in servers located within Germany (§113b). Any data localisation requirements that existed in EU Member State law have been lifted following the entry into force of the GDPR, as well as EU Regulation 2018/1807 of 28 November 2018 on the free flow of non-personal data. Germany has adjusted the German legal framework to the GDPR by passing the new German Federal Data Protection Act (Bundesdatenschutzgesetz – 'BDSG'). The BDSG was officially published on July 5, 2017 and came into force together with the GDPR on May 25, 2018. The purpose of the BDSG is especially to make use of the numerous opening clauses under the GDPR which enable Member States to specify or even restrict the data processing requirements under the GDPR.			
Greece	In Greece, the Law No. 3971/2011 goes further in the implementation of the Data Retention Directive (later annulled by the European Court of Justice) by requiring that retained data on 'traffic and localisation' stay 'within the premises of the Hellenic territory'. The Law is still in force. Any data localisation requirements that existed in EU Member State law have been lifted following the entry into force of the GDPR, as well as EU Regulation 2018/1807 of 28 November 2018 on the free flow of non-personal data. The main set of data protection rules consists of L. 2474/1997, which harmonized the Greek legislation with Directive 95/46/EC. This law sets out the obligations of those who process personal data and the respective rights of those to whom the data processing relates. The same Law also provides for the establishment of the Hellenic Data Protection Authority (HDPA) and its powers and competencies A bill of law (the 'Bill') was published on February 20, 2018 which was submitted to public consultation. It should be noted that such Bill provides for both the legal measures implementing the Regulation 2016/679 (GDPR) in Greece, as well as the integration into the Greek legal order Directive 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data. However the Bill has not been enacted yet. The Greek law 4624/2019 was enacted on August 29, 2019 (Government Gazette 137/A/29-8-2019) and provides for both the legal measures implementing the Regulation 2016/679 (GDPR) in Greece, as well as the integration into the Greek legal order of Directive 2016/680 on the protection of natural persons	Multiple data types	Across all sectors	Active

Country	DL Measure	Scope of Data Types	Scope of Sectors Affected	Status
	with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data. The Greek law includes provisions which supplement or deviate from the GDPR, especially by introducing specific rules for particular processing situations (e.g. data processing by public authorities, employment context, national security, etc.), provisions regarding criminal sanctions and the operation of the Hellenic Data Protection Authority, while retaining certain provisions of the former law 2472/1997. [91]			
India	1. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules provide that cross-border data flows of sensitive personal data or information can be made: - provided that such transfer is necessary for the performance of a lawful contract between the body corporate (or any person acting on its behalf) and the provider of information, or - provided that such transfer has been consented to by the provider of information.	Personal Data	Across all sectors	Active.
	2. In 2012, India enacted a "National Data Sharing and Accessibility Policy", which effectively means that government data (data that is owned by government agencies and/or collected using public funds) must be stored in local data centres. Moreover, Section 4 of the Public Records Act of 1993 already prohibited public records from being transferred out of Indian territory, except for 'public purposes'. It provides: "No person shall take or cause to be taken out of India any public records without prior approval of the Central Government: provided that no such prior approval shall be required if any public records are taken or sent out of India for any official purpose" On August 24, 2017, a Constitutional Bench of nine judges of the Supreme Court of India in Justice K.S.Puttaswamy (Retd.) v. Union of India [Writ Petition No. 494/ 2012] upheld that privacy is a fundamental right, which is entrenched in Article 21 [Right to Life & Liberty] of the Constitution. This led to the formulation of a comprehensive Personal Data Protection Bill 2018. The PDP Bill proposes to permit cross-border transfer of personal data and SPD subject to certain conditions, including data localisation and the transfer being subject to the DPA's approval.Furthermore, the PDP Bill recommends the localisation of at least one serving copy of personal data in India and that SPD will be stored only in servers located in India. The PDP Bill includes a new rule issued by the Reserve Bank of India (RBI) for payment systems providers operating in the country. Under the rule, all user data collected within the borders of the country needed to be localized within six months. The RBI said it was motivated by the need to have "unfettered supervisory accesses" to such data, given the fast-growing and increasingly technology dependent payments ecosystem in India.	Multiple data types	Across all sectors	Active
Indonesia	1. Regulation 82 states that the storing of personal data and performing a transaction with the	Personal Data	Across all	Active

91 Law in Greece - DLA Piper Global Data Protection Laws of the World

Country	DL Measure	Scope of Data Types	Scope of Sectors Affected	Status
	data of Indonesian nationals outside the Indonesian jurisdiction is restricted. This requirement appears to refer to personal data and transaction data of Indonesian nationals which is used within Indonesia and/or related to Indonesian nationals in particular. The Regulation targets "electronic systems operators for public services", whose definition remains unclear. In January 2014, the Technology and Information Ministry circulated a Draft Regulation with Technical Guidelines for Data Centers. The unclear and possibly all-encompassing definition of public services gave rise to concerns when a spokesperson was quoted as saying: "[the draft] covers any institution that provides information technology based services." Data carriers covered by these provisions, therefore, would include a wide range of actors such as cloud providers, foreign banks and mobile phone providers.		sectors	
	2. In Indonesia, data protection is covered by Law No. 11 of 2008 regarding Electronic Information and Transaction (EIT Law) and Government Regulation No. 82 of 2012 regarding the Provision of Electronic System and Transaction (Regulation 82), which went into force on 15 October 2012. Regulation 82 requires "electronic systems operators for public service" to set up a data centre and disaster recovery centre in Indonesian territory for the purpose of law enforcement and data protection. In January 2014, the Technology and Information Ministry circulated a Draft Regulation with Technical Guidelines for Data Centers. The unclear and possibly all-encompassing definition of public services gave rise to concerns when a spokesperson was quoted saying: "[the draft] covers any institution that provides information technology-based services." Data carriers covered by these provision, therefore, would include a wide range of actors such as cloud providers, foreign banks and mobile phone providers.	Multiple data types	Across all Sectors	Active
	3. In the Annex of Circular Letter of Bank Indonesia No. 16/11/DKSP Year 2014 regarding E-money Operations, there is a requirement for all operators of e-money to localise data centres and data recovery centres within the territory of Indonesia. A new draft Bill on the Personal Data Protection Act (PDP) being discussed and as of this date it has not been issued. Although the exact date remains uncertain and the Bill is still to be considered by the House of Representatives, if passed, this will become Indonesia's first comprehensive law to specifically deal with the issue of data privacy.	Financial Data	Specific Sector	Active
Iran	Iran does not have an explicit personal data-protection act, but it has been slowly moving toward developing its own national intranet—the Halal Internet—to separate itself (as best it can) from the rest of the Internet, including moves toward greater data localisation. Iran's government operates an extensive online censorship regime. During political protests in 2009, Iran blocked Facebook, Twitter, and YouTube. In 2015, Iran launched its own search engines, which only show approved websites. In August 2016, Iran set up its first government-paid cloud data center. In May 2016, Iran ordered foreign messaging apps, such as WhatsApp and Telegram, to store data from Iranian users locally. Iran has not enacted comprehensive data protection legislation.	Messaging and Communcaitions Data	Specific Sector	Active

Country	DL Measure	Scope of Data Types	Scope of Sectors Affected	Status
Kazakhstan	Since 2005, Kazakhstan has required that all domestically registered domain names (i.e., those on the ".kz" top-level domain) operate on physical servers within the country). Furthermore, in 2015, Kazakhstan enacted an amendment to its personal data-protection law that requires owners and operators collecting and using personal data to keep such data in-country. The requirement for localisation of personal data applies to companies established in Kazakhstan and individual proprietors in Kazakhstan, including branches and representative offices of foreign companies. It is not clear whether the localisation requirement should apply to foreign companies without any legal presence in Kazakhstan but whose websites are accessible in Kazakhstan.	Multiple data types	Across all sectors	Active
Kenya	In June 2016, Kenya released its draft National Information and Communications Technology Policy, which aims to update the government's efforts to revise ICT-related economic policy. In the section on data centers, under the title of policy objectives, the report states that policy should "facilitate the development and enactment of legislation to support growth in IT service consumption—as an engine to spur data center growth." The current updated draft legislation is said to have specific provisions on data localisation. There are various legal sources that address data protection including the Health Act 2017 and the Computer Misuse and Cybercrimes Act 2018.	Multiple data types	Across all sectors	Proposed.
Luxembourg	According to the Circular CSFF 12/552, financial institutions in Luxembourg are required to process their data within the country. Processing abroad is exceptionally permitted for an entity of the group to which the institution belongs or with explicit consent. Any data localisation requirements that existed in EU Member State law have been lifted following the entry into force of the GDPR, as well as EU Regulation 2018/1807 of 28 November 2018 on the free flow of non-personal data. Two Luxembourg Data Protection Laws of August 1, 2018 have been enacted to implement the GDPR. The first law (the Luxembourg Data Protection Law) defines the organisation of the Luxembourg data protection authority (the CNPD) and provides for specific requirements or exceptions in implementation of the GDPR. it should be noted that the Luxembourg Data Protection Law specifically prohibits the processing of genetic personal data in the field of employment law and insurance. The second law (the Luxembourg Law on Criminal Data Processing) specifically relates to the protection of individuals with regard to the processing of personal data in criminal matters and national security	Financial Data	Specific Sector	Active
Malaysia	The Personal Data Protection Act (PDPA) does not permit a data user to transfer any personal data out of Malaysia. However, the Act offers a set of exceptions, permitting the transfer of data abroad under certain conditions. The transfer is allowed if: - the data subject has given his consent to the transfer; - the transfer is necessary for the performance of a contract between the data subject and the data user; - the transfer is necessary for the conclusion or performance of a contract between the data user and a third party that is either entered into at the request of the data subject or in his interest; - the transfer is in the exercise of or to defend a legal right; - the transfer mitigates adverse actions against the data subjects; - reasonable precautions and all	Personal data	Across all sectors	Active. The law is in force, however, data need not be localised under specific conditions.

Country	DL Measure	Scope of Data Types	Scope of Sectors Affected	Status
	due diligence to ensure compliance to conditions of the Act were taken; or - the transfer was necessary for the protection the data subject's vital interests or for the public interest as determined by the Minister. While officially entered into force in November 2013, the PDPA has not yet been enforced. However, Malaysia is planning to amend its data protection laws to introduce a data breach notification regime and a wide expansion of the rights of data subjects. The Communications and Multimedia Minister has stressed the need for a refresh of the legislation, in a process that should take the EU's General Data Protection Regulation (GDPR) into consideration.			
The Netherlands	Localisation requirements apply to public records that have to be stored in archives in specific locations in the Netherlands. This applies both to paper and electronic records. Any data localisation requirements that existed in EU Member State law have been lifted following the entry into force of the GDPR, as well as EU Regulation 2018/1807 of 28 November 2018 on the free flow of non-personal data. The Dutch GDPR Implementation Act (*Uitvoeringswet AVG*, the Implementation Act) constitutes the local implementation of the GDPR in the Netherlands. The Implementation Act follows a policy-neutral approach, meaning that the requirements of the previous Dutch Data Protection Act (*Wet bescherming persoonsgegevens*) are maintained insofar as possible under the GDPR. The Implementation Act provides for, among other things, national rules where this is necessary for the implementation of GDPR provisions on the position of the regulatory authority or the fulfilment of discretionary powers provided by the GDPR.	Public Records	Across all sectors	Active.
Nigeria	1. At the beginning of 2014, the National Information Technology Development Agency (NITDA) released guidelines on Nigerian content development in information and communications technology. One of the requirements imposes that "Data and Information Management Firms" host government data locally within the country and shall not for any reason host any government data outside the country without an express approval from NITDA and the Secretary of Federal Government. Another requirement imposes that all ICT companies host their subscriber and consumer data locally.	Multiple data types	across all sectors	active
	2. The Guidelines on Point-of-Sale Card Acceptance Services require IT infrastructure for payment processing to be located domestically. All Point-of Sale and ATM domestic transactions need to be processed through local switches and it is forbidden to route transactions outside the country for processing. NITDA issued the Nigeria Data Protection Regulation 2019 ("The Regulation") on 25th January, 2019. It was enforced on the same day. The Regulation regulates the activities of Data Controllers and Data Administrators in their use of the personal data of all natural persons who are Nigerian citizens (Nigerian Citizens) or who live in Nigeria (Nigerian Residents) and several concepts have drawn precedents from the GDPR. Personal data may only be processed if at least one of five legal bases are met: (1) the data subject provides consent, or if the processing is necessary; (2) for the performance of a contract; (3) to meet a legal obligation; (4) to protect the vital interests of the data subject; or (5) for the performance of a task carried out in the public interest. Transfer of personal data outside Nigeria is allowed only if certain	Financial Data	Specific Sector	active

Country	DL Measure	Scope of Data Types	Scope of Sectors Affected	Status
	specified criteria is met. The Federal Competition and Consumer Act 2019 was enacted on February 6, 2019. Section 34(6) of the Act requires the Commission to protect the business secrets of all parties involved in Commission investigations. Section 33(2) requires Commission hearings to take place in public, but the Commission may, particularly to preserve business secrets, conduct hearings in camera.			
New Zealand	1. New Zealand's Inland Revenue Service issued a "Revenue Alert" stating that companies were required to store business records in data centres physically located in New Zealand in order to comply with the Inland Revenue Acts.	Company records	across all sectors	active
	2. Consent is not required for the transfer of data to third countries, subject to compliance with the Information Privacy Principles. However, both the Privacy Act and the Health Information Privacy Code continue to apply to personal information and health information even when it is transferred out of New Zealand. The Privacy Commissioner is given the power to prohibit a transfer of personal information from New Zealand to another state, territory, province or other part of a country by issuing a transfer prohibition notice.A Privacy Amendment Bill was introduced to New Zealand's parliament in 2018 which repeals and replaces the Privacy Act 1993, as recommended by the Law Commission's 2011 review of the Act. The bill is undergoing a second reading in the legislature and if enacted, it will include stronger powers for the Privacy Commissioner, mandatory reporting of privacy breaches, new offenses and increased fines.	Personal Data	across all sector	Active. The law is in force, however, data need not be localised under specific conditions.
Poland	According to the Polish Gambling Act, any entity organising gambling activities is obliged to archive all data exchanged between such entity and the users in an archive device located in Poland in real time. Another restriction is the requirement that the equipment (servers) for processing and storing information and data regarding the bets and their participants must be installed and kept on the territory of a member state of the EU or EFTA. Any data localisation requirements that existed in EU Member State law have been lifted following the entry into force of the GDPR, as well as EU Regulation 2018/1807 of 28 November 2018 on the free flow of non-personal data. Two new pieces of legislation are aimed at implementing the GDPR into the Polish legal order, as well as regulating the matters in which the GDPR leaves a certain regulatory freedom for EU Member States. The first one was the draft of the PDPA which came into force on May 25, 2018 (Personal Data Protection Act of 10 May 2018 (Journal of Laws of 2018, item 1000, hereinafter referred to as the new PDPA), while the second is the draft act on the provisions implementing the new PDPA (it contains a number of amendments of sectorial regulations (hereinafter referred to as the draft of the second act). The entry into force of the draft of the second act has been delayed and, according to the latest information, the legislative procedure may not be completed before late 2019. The new PDPA establishes a new supervisory body – the President of the Office for Personal Data Protection (hereinafter referred to as the President of the Office), which has a much wider range of powers than the previous DPA (Inspector General for the Protection of Personal Data – hereinafter referred to as the Inspector General). The Personal Data Protection act was further amended on 4th May 2019. As per the amendments, the Polish DPA will obtain additional powers: the DPA will be able to demand from the controller any information	Gaming Data	Specific Sector	active

Country	DL Measure	Scope of Data Types	Scope of Sectors Affected	Status
	necessary to determine the basis for calculating the penalty. The scope of required information will be determined by the DPA, who may request, for example, financial data of the company. Also, the controller will be allowed to appoint a deputy data protection officer (DPO) for periods of absence of the designated DPO. The amendments to the sectorial regulations included in the Implementing act affected, among others, employment, banking and insurance regulations. The act has been passed on February 21, 2019 and entered into force on May 4, 2019.			
Romania	1. In Romania, the game server must store all data related to the provision of remote gambling services, including records and identification of the players, the stakes placed and the winnings paid out. Information must be stored using data storage equipment (mirror server) situated on Romanian territory.	Gaming Data	Specific Sector	active
	2. In Romania, any transfer of personal data to any state requires prior notification to the National Supervisory Authority for Personal Data Processing (NSAPDP). Moreover, any transfer of personal data to a recipient state not offering an adequate level of protection needs prior approval. Any data localisation requirements that existed in EU Member State law have been lifted following the entry into force of the GDPR, as well as EU Regulation 2018/1807 of 28 November 2018 on the free flow of non-personal data. Law no. 190/208 published and applicable on July 31, 2018 constitutes the application of the GDPR into legal order. Law no. 190/2018 regulates, among others, the following activities, in addition to providing a framework related to the sanctions applicable to public authorities and public bodies: Processing of genetic data, biometric data or health data ; Processing of a national identification number ; Processing of personal data in the context of employment relationships ; Processing of personal data and of special categories of personal data within the performance of a task carried out in the public interest.	Personal Data	Across all sectors	active
Russia	1. Russian data protection has been covered since 27 July 2006 by Federal Law no. 152-FZ, also known as the OPD-law ("On Personal Data"). In July 2014, the law was amended by the Federal Law No. 242- FZ to include a clear data localisation requirement. Article 18 §5 requires data operators to ensure that the recording, systematisation, accumulation, storage, update/amendment and retrieval of personal data of the citizens of the Russian Federation is made using databases located in the Russian Federation. This amendment entered into force on 1 September 2015. It is not clear how restrictive the data localisation requirement is, but it appears that the OPD-Law does not prohibit accessing the servers from abroad and does not impose any special restriction on cross border data transfers or duplication of personal data. Online websites that violate the prohibition could be placed on the Roscomnadzor's blacklist of websites.	Personal Data	Across all sectors	Active
	2. The amendments to the National Payment System Law require international payment cards to be processed locally. The law requires international payment systems to transfer their processing capabilities with respect to Russian domestic operations to the local state-owned	Financial Data	Specific Sector	Active

Country	DL Measure	Scope of Data Types	Scope of Sectors Affected	Status
	operator (National Payment Card System) by 31 March 2015. The amendments are reported to be a response to the international political sanctions which prohibited certain international payment systems (e.g., Visa and MasterCard) from servicing payments on cards issued by sanctioned Russian banks.			
	3. The "Blogger's law" requires "organizers of information distribution in the Internet" (it is not clear which operators fall under this definition) to store on Russian territory information on facts of receiving, transfer, delivery and/or processing of voice information, texts, images, sounds and other electronic messages and information about users during six months from the end of these actions. Blogs with more than 3,000 readers are required to register as "organizers of information distribution" and are therefore subject to this requirement. Platforms that do not comply with these requirements upon a second notice face a fine of 500,000 rubles (approx. 900 USD) and can be blocked in Russia by Roscomnadzor. Russian services such as VKontakte, Yandex and Mail.Ru already registered their activities.	Multiple data types	Across all sectors	Active
	4. The Russian Government has given instructions to require public Wi-Fi user identification. The government decrees require that: - ISPs should identify Internet users, by means of identity documents (such as a passport); - ISPs should identify terminal equipment by determining the unique hardware identifier of the data network; - all legal entities in Russia are required to provide ISPs monthly with the list of the individuals that connected to the Internet using their network. The data should be stored locally for a period of at least six months. Later in 2015, the authorities proposed the following levels of fines for non-compliance: - 5,000-50,000 rubles (approx. 60-140 USD) for individual entrepreneurs; and - 100,000-200,000 rubles (approx. 1,400-2,600 USD) for legal entities. The fines would be higher for repeat offenders.	Multiple data types	across all sectors	Active
	5. According to the Federal Law no. 152-FZ "On Personal Data" (OPD-Law) the transfer of data outside Russia does not require additional consent from the data subject only if the jurisdiction that the personal data is transferred to ensures adequate protection of personal data. Those jurisdictions are parties to the Convention 108 and other countries approved by the Russian Federal Service for Supervision in the sphere of Telecom, Information Technologies and Mass Communications (Roskomnadzor). Roskomnadzor's official list of countries includes Australia, Argentina, Canada, Israel, Mexico and New Zealand. Russia's data localization legislation is officially known as Federal Law No. 242-FZ. It requires all domestic and foreign companies to accumulate, store, and process personal information of Russian citizens on servers physically located within Russian borders. Any organization that stores the information of Russian nationals, whether customers or social media users, must move that data to Russian servers. Federal Law No 374-FZ, signed in July 2016, requires local storage of information confirming the fact of receipt, transmission, delivery and/or processing of voice data, text messages, pictures, sounds, video or other communications (i.e., metadata reflecting these communications). The			

Country	DL Measure	Scope of Data Types	Scope of Sectors Affected	Status
	storage period is of three years (with respect to telecom providers) or one year (with respect to ISPs and message exchange services). In addition, local storage for a period of six months is required for the content of communications, including voice data, text messages, pictures, sounds, video or other communications. While the first requirement entered into force in July 2016, the second requirement came into force starting from July 2018.			
South Korea	1. Korea imposes a prohibition to store high resolution imagery and related mapping data outside the country and justifies this restriction on security grounds. It is reported that the prohibition led to a competitive disadvantage for international online map services, since their locally-based competitors are able to provide several services (such as turn-byturn driving/walking instructions, live traffic updates, interior building maps) that international service providers cannot.	Mapping Data	Specific Sector	Active
	2. The Personal Information Protection Act (PIPA) enacted effective as of 30 September 2011, requires companies to obtain consent from data subjects prior to exporting their personal data. The legislative bills for the amendment of Personal Information Protection Act ("PIPA") are still pending at the National Assembly. Some of the key provisions in these bills include: (a) introduction of the concept of "anonymized" personal information, for the purpose of allowing the use anonymized personal information for commercial or research purposes; (b) permitting the collection and use of personal information without the consent of the data subject when the data subject has publicly disclosed his/her personal information; and (c) limiting the scope of "personal information" by limiting the scope of information that may be combined with other personal information to be used to "identify" an individual.	Personal Data	Across all sectors	Active. The law is in force, however, data need not be localised under specific conditions.
	3. If a user's personal information is transferred to an overseas entity, the Network Act requires online service providers to disclose and obtain the user's consent, regarding the following: the specific information to be transferred overseas, the destination country, the date, time, and method of transmission, the name of the third party and the contact information of the person in charge of the personal information held by the third party, the third party's purpose of use of the personal information and the period of retention and use.	Personal Data	Across all sectors	Active. The law is in force, however, data need not be localised under specific conditions.
	4. Despite provisions in its FTAs with EU and US to allow financial data to be sent across borders, Korea prohibited outsourcing of data-processing activities to third parties in the financial services industry for several years and today certain restrictions still apply. Banks can therefore only process financial information related to Korean customers in-house, either in Korea or abroad and offshore outsourcing is restricted to a financial firm's head office, branch or affiliates. In June 2015, the Korea Financial Services Commission proposed revisions to its outsourcing policies by eliminating its requirements for (1) prior approval for the outsourcing of IT facilities; (2) offshore outsourcing to be restricted to a financial firm's head office, branch or affiliates (thus permitting use of third parties); and (3) use of a standardized outsourcing contract form (thus permitting customised contracts provided they include certain obligatory terms). Such revisions were implemented in July 2015. Yet, certain conditions for processing abroad still apply today.	Financial Data	Specific Sector	Active. The law is in force, however, data need not be localised under specific conditions.

Country	DL Measure	Scope of Data Types	Scope of Sectors Affected	Status
	Act on Promotion of Information and Communications Network Utilisation (the Network Act): If a user's personal information is transferred to an overseas entity, the Network Act requires online service providers to disclose and obtain the user's consent, regarding the following: the specific information to be transferred overseas, the destination country, the date, time, and method of transmission, the name of the third party and the contact information of the person in charge of the personal information held by the third party, the third party's purpose of use of the personal information and the period of retention and use. This act has been recently amended. Passed on August 30, 2018, amendment to the Network Act will require certain offshore information communication service providers which do not have an address or place of business in Korea, to appoint a local representative responsible for Korean data privacy compliance. This amendment will come into effect on March 19, 2019. Financial Holding Company Act (FHCA): Despite provisions in its FTAs with EU and US to allow financial data to be sent across borders, Korea prohibited outsourcing of data-processing activities to third parties in the financial services industry for several years and today certain restrictions still apply. Banks can therefore only process financial information related to Korean customers in-house, either in Korea or abroad and offshore outsourcing is restricted to a financial firm's head office, branch or affiliates. In June 2015, the Korea Financial Services Commission proposed revisions to its outsourcing policies by eliminating its requirements for (1) prior approval for the outsourcing of IT facilities; (2) offshore outsourcing to be restricted to a financial firm's head office, branch or affiliates (thus permitting use of third parties); and (3) use of a standardized outsourcing contract form (thus permitting customized contracts provided they include certain obligatory terms). Such revisions were implemented in July 2015. Yet, certain conditions for processing abroad still apply today. On 9 January 2020, the Korean National Assembly passed amendments (collectively, the 'Amendments') to three major data privacy laws: the Personal Information Protection Act ('PIPA'), the Act on the Promotion of Information and Communications Network Utilization and Information Protection ('Network Act') and the Act on the Use and Protection of Credit Information ('Credit Information Act'). [92]			
Sweden	1. In Sweden, documents such as a company's annual reports, balance sheets and annual financial reports must be physically stored in Sweden for a period of seven years.	Company Records	Across all sectors	Active.
	2. In relation to specific government authorities, there are certain provisions which might require the data processed by the authority to be held within Sweden or within the authority. This might affect the supply of cloud computing to public authorities.	Government Data	Across all sectors	Active.
	3. The Financial Services Authority requires 'immediate' access to data in its market supervision which, according to business, the supervisory body interprets as being given physical access to servers. Accordingly, Swedish financial services providers are de facto required to maintain all their records inside Swedish jurisdiction. Any data localisation requirements that existed in EU Member State law have been lifted following the	Financial Data	Specific Sector	Active

92 Korea Introduces Major Amendments To Data Privacy Laws - Privacy - South Korea

Country	DL Measure	Scope of Data Types	Scope of Sectors Affected	Status
	entry into force of the GDPR, as well as EU Regulation 2018/1807 of 28 November 2018 on the free flow of non-personal data. The Data Protection Act (2018:218) and the Data Protection Ordinance (2018:19) (the "DPA") - The DPA regulates general aspects of data protection where the GDPR allows, e.g. processing of social security numbers and processing of data pertaining to criminal offences. The DPA entered into force on 25 May 2018. In addition to the Swedish DPA, a vast number of sector specific acts have been adopted in Sweden, for example relating to the sectors of healthcare, finance, energy, environment, education, referendums/elections, enterprise, communication, labour market, etc. On 4 April 2018 in a draft to a proposal to the Council on legislation relating to personal data for scientific research purposes, the Swedish government criticised the proposal for a new scientific research data act, meaning that an update of other acts (such as the Ethical Review Act) will be enough in order to complement the GDPR. As a result of this the Swedish parliament in November 2018 voted in favor of the proposed amendments to acts relating to the processing of personal data for scientific research purposes, which did not include the adoption of a new scientific research data act. The amendments to the relevant acts entered into force on 1 January 2019.			
Taiwan	1. The transfer of personal information to mainland China is prohibited.	Personal data	Across all sectors	Active
	2. There is no consent requirement for transfer in third countries, but the data subject has to be notified in advance that his/her personal data is being transferred to another country. Yet, according to Article 21 of the Personal Data Protection Act (PDPA), the international transmission of personal information can be interrupted by the central competent government authority if the transmission involves major national interests or if the country receiving personal information lacks adequate data protection laws.	Personal Data	Across all sectors	Active. The law is in force, however, data need not be localised under specific conditions.
	3. The Financial Supervisory Commission (FSC) established stringent rules for processing of personal financial information off-shore. Yet, on May 2014, the requirements that both local and foreign banks establish standalone onshore data centres were lifted.	Financial Data	Specific Sector	Discontinued.
Turkey	1. Article 23 of Law No. 6493 requires that “the system operator, payment institution and electronic money institution shall be required to keep all the documents and records related to the matters within the scope of this Law for at least ten years within the country, in a secure and accessible manner”. The article also specifies that “the information systems and their substitutes, which are used by system operator to carry out its activities shall also be kept within the country”.	Financial Data	Specific Sector	Active
	2. The legislation stipulates that data cannot be processed or transferred abroad without the individual’s explicit consent. Consent will not be required if the transfer is necessary to exercise a right or is required by law, and either: - Sufficient protection exists in the transferee country, or - if the data controller gives a written security undertaking and Turkey’s Data Protection Board grants permission.	Personal Data	Across all sectors	Active. The law is in force, however, data need not be localised under specific conditions.
	3. The transfer of traffic and location data abroad is permitted with the data subjects’ explicit	Personal data	Across aall	Active

Country	DL Measure	Scope of Data Types	Scope of Sectors Affected	Status
	consent. There exist several regulations that try to implement various facets of LPPD. The important ones are mentioned below:176 Regulation on the Erasure, Destruction and Anonymizing of Personal Data (published in the Official Gazette dated October 28, 2017, numbered 30224) Regulation on the Working Procedures and Principles of Personal Data Protection Board (published in the Official Gazette dated November 16, 2017, numbered 30242) Regulation on the Registry of Data Controllers (published in the Official Gazette dated December 30, 2017, numbered 30286) Regulation on the Organization of Personal Data Protection Authority (published in the Official Gazette dated April 26, 2018, numbered 30403) The Communiqué on Procedures and Principles for Compliance with the Obligation to Inform (published in the Official Gazette dated March 10, 2018, numbered 30356) The Decision of Data Protection Board, dated January 31, 2018, numbered 2018/10 on Adequate Measures to be taken by Data Controllers in Processing the Special Categories of Personal Data		sectors.	
United Kingdom	According to the Companies Act 2006, "if accounting records are kept at a place outside the United Kingdom, accounts and returns (...) must be sent to, and kept at, a place in the United Kingdom, and must at all times be open to such inspection". Alongside the GDPR, the United Kingdom has prepared a new national data protection law, the Data Protection Act 2018 ("DPA"), which came into force on 25 May 2018. As well as containing derogations and exemptions from the position under the GDPR in certain permitted areas, the DPA also does the following: allows for the continued application of the GDPR in UK national law once the UK leaves the European Union (expected to be 29 March 2019); Part 3 of the DPA transposes the Law Enforcement Directive ((EU) 2016/680) into UK law, creating a data protection regime specifically for law enforcement personal data processing; Part 4 of the DPA updates the data protection regime for national security processing; and Parts 5 and 6 set out the scope of the Information Commissioner's mandate and her enforcement powers, and creates a number of criminal offences relating to personal data processing. Two sets of regulations, The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 and The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) (No. 2) Regulations 2019 have been promulgated which were made pursuant to the EU (Withdrawal) Act 2018 (EUWA). These will come into force upon UK's withdrawal from EU. Broadly speaking, these regulations are intended to preserve the status quo post-Brexit by (1) amending certain provisions of the GDPR to allow it to be retained as UK domestic law and (2) transitionally adopting certain key decisions of the EU institutions that, collectively, would allow for the continued lawfulness of personal data flows out of the United Kingdom where currently permitted under EU law The GDPR entered into force in the United Kingdom on 25 May 2018, at which point the UK was a full Member State of the European Union. The UK leaves the European Union on 31 January 2020. Whilst the UK will formally cease to be a Member State at that time, the EU – UK Withdrawal Treaty provides	Company Records	Specific Sector	Active.

Country	DL Measure	Scope of Data Types	Scope of Sectors Affected	Status
	for a transition period lasting until the end of 2020 (unless extended by joint agreement). During the transition period, EU law (including the GDPR) continues to apply directly to the UK, and the UK will be treated as if it were a Member State for the purposes of that law. Following the end of the transition period, subject to the terms of any future trade agreement reached between the EU and the UK, EU law will cease to apply in the UK. The UK Government will implement the GDPR into UK national law (creating the "UK GDPR"), subject to a number of technical changes (e.g. to amend references to "Member State" to the "United Kingdom") made under the Data Protection Act 2018, the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019. [93]			
United States	It is reported that foreign communications infrastructure providers have been asked to sign Network Security Agreements (NSAs) in order to operate in the US. These agreements ensure that U.S. government agencies have the ability to access communications data when legally requested. The agreements reported range in date from 1999 to 2011 and involve a rotating group of government agencies including the Federal Bureau of Investigation (FBI), Department of Homeland Security (DHS), Department of Justice (DoJ), Department of Defense (DoD) and sometimes the Department of the Treasury. According to the Washington Post, the agreements require companies to maintain what amounts to an "internal corporate cell of American citizens with government clearances" ensuring that "when U.S. government agencies seek access to the massive amounts of data flowing through their networks, the companies have systems in place to provide it securely". Moreover, the agreements impose local storage requirements for certain customers data as well as minimum periods of data retention for data such as billing records and access logs. The US also has hundreds of privacy and data security among its 50 states and territories, such as requirements for safeguarding data, disposal of data, privacy policies, appropriate use of Social Security numbers and data breach notification. California alone has more than 25 state privacy and data security laws, including the recently enacted California Consumer Privacy Act of 2018 (CCPA), effective January 1, 2020. The CCPA applies cross-sector and introduces sweeping definitions and broad individual rights, and imposes substantial requirements and restrictions on the collection, use and disclosure of *personal information*, which is very broadly defined as explained later in this chapter. A number of other US states are also currently proposing and considering state-level privacy legislation; in general, such legislation is similar to the CCPA in some ways, but also includes some additional or materially different requirements. Thus, it is highly possible that additional state-level privacy laws will be enacted in the US that impose requirements that go beyond or are materially different from those of the CCPA.While support is growing for a comprehensive, national privacy law that would supersede and preempt state privacy laws, it is unlikely such a law will be adopted in 2020. [94]	Multiple data types	Across all sectors	Active. However further information on this is limited.

93 Data Protection Law United Kingdom

94 Law in United States - DLA Piper Global Data Protection Laws of the World

Country	DL Measure	Scope of Data Types	Scope of Sectors Affected	Status
Vietnam	1. The Decree No. 72 entered into force in September 2013 establishes local server requirements for online social networks, general information websites, mobile telecoms network based content services and online games services. All these organisations are required to establish at least one server inside the country "serving the inspection, storage, and provision of information at the request of competent state management agencies". The Government of Vietnam recently issued Decree No. 27/2018/ND-CP ("Decree No. 27") to amend and supplement Decree No. 72/2013/ND-CP dated 15 July 2013 on the management, provision, and use of Internet services and online information ("Decree No. 72"). Decree No. 27 took effect on 15 April 2018. Aggregated information websites and social networks are required to set up a warning mechanism in case their members post illegal content (filter). In the event of illegal content being posted on their platforms, aggregated information websites and social networks must have a coordinating mechanism to remove illegal content within three (3) hours after the aggregated information websites and social networks discover such illegal content or receive takedown requests from the MIC or licensing authorities via written documents, telephone or email.	Multiple data types	Across all sectors	Active. Comes into force in January 2019
	2. According to the Decree 90 of 2008, advertising service providers that use email advertisements and internet based text messages are required to send emails from a Vietnamese domain name (".vn") website which is operated from a server located in Vietnam. 3.On June 12, 2018, the Vietnamese National Assembly passed the Law on Cybersecurity (the "Cybersecurity Law"), which was enforced on January 1, 2019. Among other aims, the law seeks to regulate data processing methods of technology companies that operate in Vietnam and restrict the internet connections of users who post "prohibited" content. The Cybersecurity Law will, in principle, affect both domestic and foreign companies that provide services through telecommunication networks or the internet, or value-added services to customers in Vietnam. Interpreted broadly, these services would include social networks, search engines, online advertising, online broadcasting and streaming, e-commerce websites and marketplaces, internet-based voice/text services (OTT services), cloud services, online games and other online applications. The Cybersecurity Law will be required to store the personal data of Vietnamese end-users in Vietnam for the legally prescribed period of time, and surrender such data to Vietnamese government authorities upon request. Foreign companies providing telecommunications or internet services in Vietnam must: Establish offices in Vietnam Store the personal information of Vietnamese users and "other important data" in Vietnam and perform a security assessment prior to any cross-border data transfer; Bring their technology products involving cyber services into compliance with "quality assurance" standards before they can be released to the market. It also requires administrators of information systems critical to national security to store personal data and "critical data" within the national territory of Vietnam. It is unclear when an information system develops to a point that it is critical to national	Domain Data	Specific Sector	Active

Country	DL Measure	Scope of Data Types	Scope of Sectors Affected	Status
	security. Neither is it clear whether the systems cover state-owned systems only or include private systems as well. "Critical data" is also not defined.			
Venezuela	Venezuela has passed regulations requiring that IT infrastructure for payment processing be located domestically. The Constitutional Chamber of the Supreme Court of Justice has acknowledged the possibility that a person or entity may collect and maintain information on individuals and their goods/purchases, arranged in such way that a profile of individuals, their activities, or their goods can be made, with the purpose of using them for the benefit of the collecting entity or of third parties, provided that all constitutional rights are respected, and in particular the ones established in Article 28 of the Constitution. Whoever collects and records information on individuals and their goods, must respect the right of every person to protect his honor, private life, intimacy, self-image, confidentiality and reputation, which is granted in Article 60 of the Constitution.Also, in accordance with a binding decision of the Constitutional Chamber, any person who collects and manages personal information must guarantee the following principles: ● Principle of free will ● Principle of legality ● Principle of purpose and quality ● Principle of temporality or conservation ● Principle of accuracy and self-determination ● Principle of security and confidentiality ● Principle of guardianship ● Principle of responsibility (collectively called the 'Principles'). There are also specific provisions concerning data protection with limited scope of application, contained in the Banking Institutions Law and the Special Law against Cybercrime. [95]	Financial Data	Specific Sector	Active

Source: Compiled by authors from ITIF, ECIPE, DLA Piper and other secondary sources

95 Data Protection Law Venezuela

Appendix 2

Table A2.1: Complete Table of Indicators

Countries	General Economy Indicators						Digital Economy Indicators						State Capacity Indicators						
	Income Level (2020)	GDP Per Capita (PPP, Current International $) (2018)	Unemployment Rate (% of total labour force) (2019)	Current Account Balance (in billions of US Dollars) (2018)	Current Account Balance (% of GDP) (2020)	Foreign Direct Investment, net inflows (% of GDP) (2018)	International Internet Bandwidth per Internet User (kbits/s) (June 2018)	Percentage of Individuals Using the Internet (2018)	Fixed - Broadband Subscriptions per 100 Population (2018)	Mobile Cellular Subscriptions per 100 Population (2018)	Mobile Broadband Subscribers per 100 Population (June 2018)	Secure Internet Servers (per 1 million people) (2018)	Regime Type	Political Stability and Absence of Violence (2018)	Government Effectiveness (2018)	Regulatory Quality (2018)	Rule of Law (2018)	Control of Corruption (2018)	Government Net Lending/Borrowing (% of GDP) (2020)
Afghanistan	Low Income	1955	11.10	-3.654	4.9	0.6	11.6	12.78	0.04	59.12	16	53	Authoritarian	-2.75	-1.46	-1.13	-1.67	-1.50	-0.04
Algeria	Upper Middle Income	15481.8	11.70	-22.058	-18.3	0.9	25.4	49.04	7.26	111.66	78.4	68	Hybrid Regime	-0.79	-0.44	-1.26	-0.78	-0.64	-0.15
Australia	High Income	51663.40	5.30	-29.660	-0.6	4.20	67.60	89.91	30.69	113.58	134.90	32,891.00	Full Democracy	0.98	1.60	1.93	1.72	1.81	-0.097
Bahrain	High Income	47303	0.70	-2.434	-9.6	0.3	108.8	98.64	11.76	133.34	147.3	371	Authoritarian	-0.84	0.18	0.45	0.41	-0.15	-0.157
Bangladesh	Lower Middle Income	4371.8	4.20	-7.593	-2.2	1.1	15.3	18.68	6.34	100.24	30	116	Hybrid Regime	-1.03	-0.75	-0.83	-0.64	-0.91	-0.064
Belgium	High Income	51408.00	5.60	-5.250	-0.7	-11.60	135	88.66	39.22	99.70	75.10	13,979.00	Flawed Democracy	0.41	1.17	1.23	1.37	1.51	-0.089
Bhutan	Lower Middle Income	10167.9	2.30	-0.497	-21.3	0.1	18.2	50.69	1.43	93.26	87.4	178	Hybrid Regime	1.10	0.36	-0.33	0.55	1.65	-0.055
Bolivia	Lower Middle Income	7873.2	3.50	-1.989	-4.6	0.6	39.2	44.29	4.44	100.82	76.5	130	Hybrid Regime	-0.24	-0.32	-0.89	-1.15	-0.63	-0.073
Brazil	Upper Middle Income	16096.40	12.10	-41.539	-1.8	4.20	29	70.43	14.91	98.84	90.20	2,036.00	Flawed Democracy	-0.36	-0.45	-0.31	-0.28	-0.42	-0.093
Bulgaria	Upper Middle Income	21960.40	4.30	3.492	1.7	1.90	215	64.78	27.00	118.94	91.60	38,228.00	Flawed Democracy	0.42	0.27	0.58	-0.03	-0.15	-0.029
Canada	High Income	48130.30	5.60	-45.322	-3.7	2.70	74	93.78	38.96	89.58	72.50	30,952.00	Full Democracy	0.99	1.72	1.67	1.77	1.87	-0.118
China	Upper Middle Income	18236.60	4.30	49.091	0.5	1.50	27.90	60.71	28.54	115.53	83.60	447.00	Authoritarian	-0.26	0.48	-0.14	-0.20	-0.27	-0.112
Colombia	Upper Middle Income	15012.90	9.70	-13.037	-4.7	3.50	157	64.13	13.45	129.91	48.80	651.00	Flawed Democracy	-0.81	-0.09	0.33	-0.41	-0.30	-0.025
Costa Rica	Upper Middle Income	17671.1	11.90	-1.866	-4.5	4.6	52.7	74.09	16.7	169.93	116.6	1206	Full Democracy	0.49	0.38	0.48	0.48	0.55	-0.078
Cyprus	High Income	38513.30	7.30	-1.067	-8.3	20.90	59	84.43	36.27	138.90	106.40	6,372.00	Flawed Democracy	0.54	0.92	1.02	0.75	0.64	-0.018
Czech Republic	High Income	39743.6	1.90	0.860	-2.1	3.5	59.3	80.69	30.22	119.11	81.9	42361	Flawed Democracy	1.04	0.92	1.26	1.05	0.50	-0.047
Denmark	High Income	55671.20	4.90	24.780	4.8	0.30	87	97.32	44.06	125.12	129.00	1,23,074.00	Full Democracy	0.96	1.87	1.68	1.83	2.15	-0.07

Countries	General Economy Indicators						Digital Economy Indicators						State Capacity Indicators						
	Income Level (2020)	GDP Per Capita (PPP, Current International $) (2018)	Unemployment Rate (% of total labour force) (2019)	Current Account Balance (in billions of US Dollars) (2018)	Current Account Balance (% of GDP) (2020)	Foreign Direct Investment, net inflows (% of GDP) (2018)	International Internet Bandwidth per Internet User (kbits/s) (June 2018)	Percentage of Individuals Using the Internet (2018)	Fixed - Broadband Subscriptions per 100 Population (2018)	Mobile Cellular Subscriptions per 100 Population (2018)	Mobile Broadband Subscribers per 100 Population (June 2018)	Secure Internet Servers (per 1 million people) (2018)	Regime Type	Political Stability and Absence of Violence (2018)	Government Effectiveness (2018)	Regulatory Quality (2018)	Rule of Law (2018)	Control of Corruption (2018)	Government Net Lending/Borrowing (% of GDP) (2020)
Egypt	Lower Middle Income	12412.3	10.80	-6.293	-4.3	2.7	16	46.92	6.69	95.29	50.1	35	Authoritarian	-1.16	-0.58	-0.87	-0.41	-0.59	-0.077
Estonia	High Income	35973.8	5.10	0.612	-2.7	3.8	123.1	89.36	33.35	145.44	133.4	48934	Flawed Democracy	0.60	1.19	1.56	1.24	1.51	-0.083
Finland	High Income	48416.90	6.60	-4.468	-3.5	-1.80	84	88.89	31.45	129.47	153.80	33,984.00	Full Democracy	0.92	1.98	1.79	2.05	2.21	-0.067
France	High Income	45342.40	8.40	-19.014	-0.7	2.20	55	82.04	44.78	108.36	87.50	20,415.00	Full Democracy	0.11	1.48	1.17	1.44	1.32	-0.092
Germany	High Income	53074.50	3.00	289.897	6.6	2.70	54	89.74	41.11	129.32	79.80	56,392.00	Full Democracy	0.60	1.62	1.75	1.63	1.95	-0.055
Ghana	Lower Middle Income	4746.7	4.30	-2.043	-4.5	4.6	10.1	39.53	0.21	137.52	83.2	22	Flawed Democracy	0.03	-0.21	-0.08	0.07	-0.11	-0.1
Greece	High Income	29592.20	17.20	-6.248	-6.5	1.80	86	72.95	37.65	115.67	63.40	5,038.00	Flawed Democracy	0.09	0.34	0.30	0.15	-0.07	-0.09
Hungary	High Income	31102.5	3.40	-0.677	-0.1	-41.5	61	76.07	31.72	103.45	49.1	19257	Flawed Democracy	0.76	0.49	0.60	0.56	0.05	-0.03
India	Lower Middle Income	7762.90	5.40	-65.599	-0.6	1.50	26	30.64	1.34	86.94	25.80	188.00	Flawed Democracy	-0.96	0.28	-0.18	0.03	-0.19	-0.074
Indonesia	Lower Middle Income	13079.60	4.70	-31.046	-3.2	1.90	21	39.90	3.32	119.34	95.70	1,283.00	Flawed Democracy	-0.53	0.18	-0.07	-0.31	-0.25	-0.05
Ireland	High Income	83203.4	4.90	40.900	6.3	16.9	78.3	84.52	29.68	103.17	102	69792	Full Democracy	1.03	1.42	1.60	1.46	1.55	-0.052
Italy	High Income	41830.4	9.90	53.839	3.1	1.9	35.7	74.39	28.14	137.47	87.9	12256	Flawed Democracy	0.31	0.41	0.67	0.25	0.24	-8.3
Japan	High Income	42797.50	2.30	174.718	1.7	0.50	25	91.28	32.62	141.41	133.20	11,671.00	Flawed Democracy	1.06	1.68	1.33	1.53	1.42	-7.1
Jordan	Upper Middle Income	9478.9	14.70	-2.849	-5.8	2.2	49.9	70.86	4.01	87.62	100	103	Authoritarian	-0.38	0.11	0.08	0.23	0.15	-6.7
Kazakhstan	Upper Middle Income	27879.80	4.60	-0.288	-6.8	0.10	70	78.90	13.44	142.28	75.10	1,374.00	Authoritarian	0.00	0.02	0.14	-0.43	-0.50	-5.3
Kenya	Lower Middle Income	3467.60	2.60	-5.018	-4.6	1.80	103	20.49	0.72	96.32	35.70	217.00	Hybrid Regime	-1.16	-0.41	-0.23	-0.41	-0.85	-7.7
Latvia	High Income	30304.9	6.50	-0.210	-2.2	1.3	132.5	83.58	27.28	107.35	117.9	14509	Flawed Democracy	0.42	1.04	1.19	0.96	0.33	-5.2
Luxembourg	High Income	113337.40	5.40	3.426	4	-7.90	8,410	97.06	37.12	132.16	88.10	43,167.00	Full Democracy	1.37	1.78	1.76	1.81	2.09	-2.8
Malawi	Low Income	1311	5.70	-1.426	-17.9	1.4	3.6	12.45	0.06	39.01	25.5	15	Hybrid Regime	-0.33	-0.73	-0.67	-0.38	-0.74	-6.3
Malaysia	Upper Middle Income	31782.2	3.30	7.590	-0.1	2.4	56.2	81.20	8.55	134.53	111.5	5713	Flawed Democracy	0.24	1.08	0.68	0.62	0.31	-4.2

Countries	General Economy Indicators						Digital Economy Indicators						State Capacity Indicators						
	Income Level (2020)	GDP Per Capita (PPP, Current International $) (2018)	Unemployment Rate (% of total labour force) (2019)	Current Account Balance (in billions of US Dollars) (2018)	Current Account Balance (% of GDP) (2020)	Foreign Direct Investment, net inflows (% of GDP) (2018)	International Internet Bandwidth per Internet User (kbits/s) (June 2018)	Percentage of Individuals Using the Internet (2018)	Fixed - Broadband Subscriptions per 100 Population (2018)	Mobile Cellular Subscriptions per 100 Population (2018)	Mobile Broadband Subscribers per 100 Population (June 2018)	Secure Internet Servers (per 1 million people) (2018)	Regime Type	Political Stability and Absence of Violence (2018)	Government Effectiveness (2018)	Regulatory Quality (2018)	Rule of Law (2018)	Control of Corruption (2018)	Government Net Lending/Borrowing (% of GDP) (2020)
Mexico	Upper Middle Income	19844.6	3.40	-21.995	-0.3	3.1	36.4	65.77	14.55	95.23	63.6	226	Flawed Democracy	-0.57	-0.15	0.15	-0.67	-0.86	-4.2
Morocco	Lower Middle Income	8611.7	9.00	-6.444	-7.8	3.1	49.8	64.80	4.31	124.17	58.3	296	Hybrid Regime	-0.33	-0.21	-0.24	-0.14	-0.22	-7.1
Mozambique	Low Income	1459.7	3.20	-4.500	-68.8	18.2	1.2	16.63	0.24	47.72	25.7	12	Authoritarian	-0.78	-0.87	-0.73	-1.04	-0.78	-7.7
Myanmar	Lower Middle Income	6674	1.60	-2.137	-4.7	1.8	6.9	29.97	0.24	113.84	75.1	9	Authoritarian	-1.31	-1.07	-0.75	-1.03	-0.59	-4.7
Namibia	Upper Middle Income	11101.8	20.30	-0.354	-0.4	1.4	13.8	40.57283504	2.53	112.7	59.3	149	Flawed Democracy	0.65	0.11	-0.05	0.24	0.34	-7
Nepal	Low Income	3089.6	1.40	-2.774	-6.5	0.2	19.8	29.318639401	2.82	139.45	52.4	182	Hybrid Regime	-0.63	-0.90	-0.75	-0.48	-0.67	-6
Netherlands	High Income	56328.9	3.20	99.065	9	-26.2	119.7	94.712073772	43.42	123.73	90.8	100585	Full Democracy	0.87	1.85	2.02	1.82	2.01	-6.2
New Zealand	High Income	41005.40	4.10	-7.708	-4.5	1.00	166	92.52	34.72	134.93	101.60	17,673.00	Full Democracy	1.54	1.67	1.98	1.88	2.17	-5.2
Nigeria	Lower Middle Income	5990.90	8.10	5.334	-3.3	0.50	3	39.17	0.04	88.18	19.90	184.00	Hybrid Regime	-2.19	-1.02	-0.88	-0.88	-1.04	-6.4
Norway	High Income	65510.6	3.30	31.372	-1.3	-4	95.3	96.49	41.34	107.17	95.1	20877	Full Democracy	1.15	1.89	1.76	1.97	2.09	0.8
Pakistan	Lower Middle Income	5567.1	4.50	-19.191	-1.7	0.7	22	15.65	0.85	72.56	24.7	109	Hybrid Regime	-2.27	-0.63	-0.64	-0.67	-0.79	-9.2
Paraguay	Upper Middle Income	13599.9	4.80	0.008	-2.2	1	19.2	64.99	4.61	106.95	47.9	248	Flawed Democracy	-0.12	-0.52	-0.12	-0.54	-0.85	-5.1
Philippines	Lower Middle Income	8951.1	2.20	-8.729	-2.3	3	18.9	66.76	3.68	126.2	68.6	93	Flawed Democracy	-1.12	0.05	0.05	-0.48	-0.54	-3.4
Poland	High Income	31336.60	3.50	-5.820	0.2	2.90	23	77.54	16.13	134.75	154.10	16,225.00	Flawed Democracy	0.55	0.66	0.88	0.43	0.64	-6.7
Portugal	High Income	33415.4	6.30	0.956	0.3	2.7	52.9	74.66	36.9	115.63	68.9	15981	Full Democracy	1.14	1.21	0.89	1.14	0.85	-7.1
Qatar	High Income	126898.4	0.10	16.652	-1.9	-1.1	90	99.65	9.63	141.86	117.4	397	Authoritarian	0.68	0.63	0.52	0.73	0.72	5.2
Romania	Upper Middle Income	28206.40	4.00	-10.944	-5.5	3.10	49.80	70.68	26.06	116.25	82.90	15,938.00	Flawed Democracy	0.06	-0.25	0.45	0.33	-0.12	-8.9
Russia	Upper Middle Income	27588.10	4.60	113.454	0.7	0.50	69	80.86	22.00	157.43	80.80	5,191.00	Authoritarian	-0.50	-0.06	-0.54	-0.82	-0.85	-4.8
Rwanda	Low Income	2251.6	1.00	-0.746	-16.2	3.2	8.7	21.57	0.06	78.85	35	36	Authoritarian	0.12	0.21	0.08	0.12	0.58	-8.1
Saudi Arabia	High Income	55335.70	5.90	70.606	-3.1	0.50	188	93.31	20.24	122.57	90.00	162.00	Authoritarian	-0.52	0.32	-0.05	0.14	0.36	-12.6
Singapore	High Income	101531.6	4.10	65.072	14.8	22.5	954.1	88.17	27.97	148.82	148.2	84714	Flawed Democracy	1.51	2.23	2.13	1.84	2.17	-3.5

Countries	General Economy Indicators						Digital Economy Indicators						State Capacity Indicators						
	Income Level (2020)	GDP Per Capita (PPP, Current International $) (2018)	Unemployment Rate (% of total labour force) (2019)	Current Account Balance (in billions of US Dollars) (2018)	Current Account Balance (% of GDP) (2020)	Foreign Direct Investment, net inflows (% of GDP) (2018)	International Internet Bandwidth per Internet User (kbits/s) (June 2018)	Percentage of Individuals Using the Internet (2018)	Fixed - Broadband Subscriptions per 100 Population (2018)	Mobile Cellular Subscriptions per 100 Population (2018)	Mobile Broadband Subscribers per 100 Population (June 2018)	Secure Internet Servers (per 1 million people) (2018)	Regime Type	Political Stability and Absence of Violence (2018)	Government Effectiveness (2018)	Regulatory Quality (2018)	Rule of Law (2018)	Control of Corruption (2018)	Government Net Lending/Borrowing (% of GDP) (2020)
Slovak Republic	High Income	33736.4	5.60	-2.760	-3	2.4	77.7	80.66	27.65	132.8	82.6	12993	Flawed Democracy	0.75	0.71	0.81	0.53	0.36	-5.9
Slovenia	High Income	38048.8	4.20	3.073	0.8	2.8	121.9	79.75	29.49	118.67	70	33122	Flawed Democracy	0.91	1.13	0.69	1.06	0.87	-6.6
South Africa	Upper Middle Income	13686.9	28.20	-13.384	0.2	1.5	17.4	68.43	1.92	159.93	70	12034	Flawed Democracy	-0.28	0.34	0.17	-0.10	-0.02	-13.3
South Korea	High Income	40111.80	4.10	76.408	4.9	0.90	69.90	96.02	41.60	129.67	112.80	2,064.00	Flawed Democracy	0.54	1.18	1.09	1.24	0.60	-1.8
Spain	High Income	39715.4	14.00	27.306	2.2	3.5	27	86.11	32.5	115.99	95.5	11321	Full Democracy	0.25	1.00	0.95	0.97	0.61	-9.5
Sri Lanka	Upper Middle Income	13473.7	4.20	-2.813	-3.6	1.8	29.5	28.51	7.27	142.65	22.4	412	Flawed Democracy	-0.18	-0.24	-0.15	0.03	-0.34	-9.4
Sweden	High Income	53208.90	6.50	9.478	2.2	1.60	67	92.14	39.85	126.83	122.60	18,594.00	Full Democracy	0.91	1.83	1.80	1.90	2.14	-5.3
Switzerland	High Income	68060.9	4.60	74.099	7.2	-9.6	80.6	91.31	46.42	126.77	99.7	68137	Full Democracy	1.34	2.04	1.78	1.93	2.01	-5.1
Thailand	Upper Middle Income	19051.3	0.80	32.385	5.2	2.7	119.5	56.82	13.24	180.18	99	954	Flawed Democracy	-0.73	0.35	0.11	0.02	-0.40	-3.4
Turkey	Upper Middle Income	28068.90	13.50	-27.032	0.4	1.70	84	71.04	16.28	97.30	70.50	4,335.00	Hybrid Regime	-1.33	0.01	-0.05	-0.32	-0.34	-7.5
Uganda	Low Income	2038.1	1.80	-2.564	-9.7	4.9	7.5	24.20	0.02	57.27	23.4	20	Hybrid Regime	-0.69	-0.61	-0.25	-0.29	-1.04	-6.8
UK	High Income	45973.60	3.90	-123.105	-4.4	1.20	422	94.90	39.60	118.37	88.10	27,250.00	Full Democracy	0.05	1.34	1.76	1.64	1.83	-8.3
Ukraine	Lower Middle Income	9249.5	8.90	-4.367	-2	1.9	77.1	62.55	12.8	127.75	41.7	6028	Hybrid Regime	-1.83	-0.42	-0.22	-0.72	-0.87	-8.2
Uruguay	High Income	23572.2	8.70	0.075	-2.5	2	109.6	74.77	28.34	149.9	112.1	1575	Full Democracy	1.05	0.56	0.50	0.60	1.27	-4.7
USA	High Income	62794.60	3.70	-490.991	-2.6	1.30	125.40	83.36	33.80	129.01	132.90	65,768.00	Flawed Democracy	0.48	1.58	1.58	1.45	1.32	-15.4
Vietnam	Lower Middle Income	7447.80	2.00	5.899	0.7	6.30	137.30	70.35	13.60	147.20	46.90	1,769.00	Authoritarian	0.20	0.00	-0.39	0.00	-0.49	-5.2

Sources: World Bank, IMF Data Mapper, ITU, ICRG, EIU Democracy Index 2019

Notes – Income Level Scores: 0 – Low Income; 1 – Lower Middle Income; 2 – Upper Middle Income; 3 – High Income

Regime Type Scores: 0 – Authoritarian; 1 – Flawed Democracy; 2 – Hybrid Regime; 3 – Full Democracy

Data Sources

Variable	Source
Income Level	https://datahelpdesk.worldbank.org/knowledgebase/articles/906519-world-bank-country-and-lending-groups
GDP Per Capita (PPP, Current International $)	https://data.worldbank.org/indicator/NY.GDP.PCAP.PP.CD
Unemployment Rate (% of total labour force)	https://data.worldbank.org/indicator/SL.UEM.TOTL.ZS
Current Account Balance (in billions of US Dollars)	https://data.worldbank.org/indicator/BN.CAB.XOKA.CD
current account balance (% of GDP)	https://www.imf.org/external/datamapper/BCA_NGDPD@WEO/FRA/GBR/DEU
Foreign Direct Investment, net inflows (% of GDP)	https://data.worldbank.org/indicator/BX.KLT.DINV.WD.GD.ZS
International Internet Bandwidth per Internet User (kbits/s)	https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2018/MISR-2018-Vol-2-E.pdf
Percentage of Individuals Using the Internet (countries for which 2018 data was not available, the values have been projected using past years' data)	https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx
Fixed - Broadband Subscriptions per 100 Population	https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx
Mobile Cellular Subscriptions per 100 Population	https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx
Mobile Broadband Subscribers per 100 Population	https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2018/MISR-2018-Vol-2-E.pdf
Secure Internet Servers (per 1 million people)	https://data.worldbank.org/indicator/IT.NET.SECR.P6?view=chart
Political Stability and Absence of Violence (2018)	https://info.worldbank.org/governance/wgi/
Government Effectiveness	
Regulatory Quality	
Rule of Law	
Control of Corrpution	
Government Net Lending/ Borrowing (% of GDP) (2020)	https://www.imf.org/external/datamapper/GGXCNL_G01_GDP_PT@FM/ADVEC/FM_EMG/FM_LIDC

Methodology

All Sub-Indices and the Digital Potential Index

The index has been created using equal weights or a simple average aggregation technique where all the sub-indices will be given equal weights and all the variables within the sub-

indices have equal weights (=1). This method of aggregation is used when there is limited/ no information to judge whether some aspects of the index are more important than the other. Even when the order of magnitude is known, the data should allow determination of a measured value of how much more one indicator / group of indicators is valued than the others. UNDP's Human Development Index and World Bank's Ease of Doing Business Index are two indices which use simple averages. To create the area wise indices, we normalised each of the variables under that area to make it a unit less index lying between 0 and 1 by using the Min-Max Transformation.

Higher values of reflects better performance. The arithmetic mean is used to aggregate the sub-indicators under each of the five areas for each of the states. We create the sub-indices (General economy, State capacity and Digital economy) for each country by taking the geometric mean to aggregate the scores across the parameters which has been considered under each index. The use of geometric mean reduces the level of substitutability between the areas and smoothens the intrinsic differences across them. While the index will draw a cross-country comparison and analyse whether there exists a correlation between the levels of development in a country's digital economy and their data localisation policies.

Scores for Restrictions to Cross-Border Data Flows

The general and sectoral restrictions to cross-border data flows across countries have been scored based on the method outlined in the tables below.

Table A2.2.1: General RCBDF Scoring Methodology

General Restrictions to Cross-Border Data Flows					
Type of Restriction	**Score**	**Type of Data**	**Score**	**Status of Law**	**Score**
Unconditional Flow of Data	0	Sensitive Personal Data	0	Proposed	0
Conditional Flow without Local Storage Requirements	1	Personal Data	1	Active	1
Mirroring Requirements	2	Non-Personal Data	2		
Conditional Flow of Data with Local Storage Requirements	3	All types of Data	3		
Ban on Transfer	4				

Table A2.2.2: Sectoral CBDF Scoring Methodology

Sector Specific Restrictions to Cross-Border Data Flows					
Number of Sectors	**Score**	**Type of Restriction**	**Score**	**Status of Law**	**Score**
None	0	Unconditional Flow of Data	0	Proposed	0
One	1	Conditional Flow without Local Storage Requirements	1	Active	1
Multiple	2	Mirroring Requirements	2		
		Conditional Flow of Data with Local Storage Requirements	3		
		Ban on Transfer	4		

Table A2.3.1: General RCBDF Scores by Country

Country	General RCBDF
Afghanistan	
Algeria	
Australia	3
Bahrain	3
Bangladesh	
Belgium	3
Bhutan	
Bolivia	0
Brazil	3
Bulgaria	3
Canada	3
China	5
Colombia	3
Costa Rica	3
Cyprus	3
Czech Republic	3
Denmark	3
Egypt	3
Estonia	3
Finland	3
France	3
Germany	3
Ghana	3
Greece	3
Hungary	3
India	4
Indonesia	5
Ireland	3
Italy	3
Japan	3
Jordan	
Kazakhstan	5
Kenya	3
Latvia	3
Luxembourg	3
Malawi	
Malaysia	3
Mexico	3
Morocco	3
Mozambique	
Myanmar	
Namibia	
Nepal	
Netherlands	3
New Zealand	3
Nigeria	3
Norway	3
Pakistan	5
Paraguay	
Philippines	3
Poland	3
Portugal	3
Qatar	3
Romania	3
Russian Federation	5

Country	General RCBDF
Rwanda	
Saudi Arabia	
Singapore	3
Slovakia	3
Slovenia	3
South Africa	3
South Korea	3
Spain	3
Sri Lanka	
Sweden	3
Switzerland	3
Thailand	3
Turkey	3
Uganda	3
UK	3
Ukraine	3
Uruguay	0
USA	0
Vietnam	5
	No Data Protection Law
	Information on restrictions to CBDF not available
	Draft law. No score has been assigned if information on any existing/ active laws that explicitly restrict CBDF is not available

Source: DLA Piper, UNCTAD, other secondary sources and author's calculations

Table A2.3.1: Sectoral RCBDF Scores by Country

Country	Sectoral RCBDF
Australia	5
Brazil	0
Canada	5
China	10
Colombia	0
Bulgaria	5
Denmark	7
Finland	5
France	5
Germany	6
Greece	5
Luxembourg	5
Netherlands	5
Poland	5
Romania	5
Sweden	6
India	10
Indonesia	6
Kazakhstan	5
Kenya	0
Malaysia	0
Nigeria	10
New Zealand	5
Russia	6
South Korea	6
Turkey	5
UK	5
Vietnam	0

Results

Correlation Tables

Table A2.4: Correlation Matrix – Digital Potential Index/ Sub-Indices and General RCBDF for all Countries

Correlation Matrix (Pearson's Correlation)	General Economy Sub-Index	Digital Economy Sub-Index	State Capacity Sub-Index	Digital Potential Index
Scores for Restrictions to Cross-Border Data Flows	-0.2121	-0.2097	-0.2435	-0.2411
	Significant at 10% level			

Correlation Matrix (Spearman's Rank Correlation)	General Economy Sub-Index	Digital Economy Sub-Index	State Capacity Sub-Index	Digital Potential Index
Scores for Restrictions to Cross-Border Data Flows	-0.2975	-0.3007	-0.3109	-0.3212
	Significant at 5% level			

Source: Author's calculations

Table A2.5: Correlation Matrix – Digital Potential Index/ Sub-Indices and General CBDF for Countries with Restrictions to Cross-Border Data Flows

Correlation Matrix (Pearson's Correlation)	General Economy Sub-Index	Digital Economy Sub-Index	State Capacity Sub-Index	Digital Potential Index
Scores for Restrictions to Cross-Border Data Flows	-0.3737	-0.307	-0.417	-0.3978
	Significant at 5% level			

Correlation Matrix (Spearman's Rank Correlation)	General Economy Sub-Index	Digital Economy Sub-Index	State Capacity Sub-Index	Digital Potential Index
Scores for Restrictions to Cross-Border Data Flows	-0.3974	-0.3562	-0.4146	-0.4136
	Significant at 5% level			

Source: Author's calculations

Appendix 3

Case Studies

This section reviews four case studies that highlight the country level experience with data localisation measures, implementing such measures. It provides the context and details of the localisation measure and the challenges and implications thereof.

Specifically, the case studies look at **Vietnam's** expansive data localisation regime, **Indonesia's** attempts to amend data localisation legislation to suit business and economic compulsions, **Australia's** health data localisation under a struggling health care records system, and **South Korea's** Spatial data localisation that witnessed strict enforcement at the backdrop of a ceasefire with North Korea.

The case studies attempt to capture the varying degrees of data localisation enforcement, and different contexts in which they have emerged: From Vietnam and Indonesia's more recent broad-based data localisation regimes, Australia's sector and system specific regime to South Korea's data-type specific regime that were in place much before the global trends picked up post the Edward Snowden disclosures.

1. Vietnam: Testing an expansive Data Localisation mandate

Data Localisation Legislation

The number of users of social networks in Vietnam is expected to grow to 44.06 million by 2022. Social, political and economic complexities arising from increasing number of users on social media compel governments to legislate on data privacy and cyber security. The objective provided by the government for the intervention is to maintain social order, and national security. The language and objective of the statue clearly attempts to quell any political discourses that were anti-state. On the 12th of June, 2018, the Vietnamese Government legislated its 'Law 24 on Cyber security' that passed with 86 percent of the members of parliament voting in its favor[96]. The law came into effect on January 1, 2019. In relation to Data Localisation, Law 24 on Cyber Security mandates the following responsibilities on any domestic or foreign enterprise that provide services on telecom networks and on the Internet and other value-added services in cyber space in Vietnam:

Under Article 26, *Guarantees relating to information security in Cyberspace*

2. a. …To provide user information to the Cyber security Task Force under the Ministry of Public Security when so requested in writing in order to serve investigation of and dealing with breaches of the law on cyber security.

2. b. To prevent the sharing of information and to delete information with the contents prescribed in clauses 1 to 5 of Article 16 of this Law on services or information systems

[96] https://e.vnexpress.net/news/news/vietnam-says-cybersecurity-law-needed-to-ensure-national-security-3762377.html

directly managed by any agency or organization no later than twenty four hours after the time of a request from the Cyber Security Task Force under the Ministry of Public Security or from a competent agency under the Ministry of Information and Communications, and to save/maintain system logs in order to serve investigation of and dealing with breaches of the law on cyber security within a (specified) period (to be) stipulated by the Government.

3. Domestic and Foreign Service providers on telecom networks and on the Internet and other value added services in cyber space in Vietnam carrying out activities of collecting, exploiting, analyzing and processing data about personal information, data about service users' relationships and data generated by service users in Vietnam must store such data in Vietnam for a period to be stipulated by the Government.

Foreign enterprise referred to in this clause must have branches or representative offices in Vietnam.

4. The Government shall provide detailed regulations on clause 3 of this article.

Implications and Challenges

Vietnam legislated its 'Law 24 on Cyber security' in June 2018, allowing entities and organizations on which the law is binding, time till January 2019 for compliance. However, an initial assessment based on the reception of this legislation and other related factors could shed light on how the law might potentially unravel over time.

As a preliminary remark, it is useful to look at Indonesia's experience with its own, expansive, initial data localisation legislation- their experience informs that compliance data localisation law that is expansive in scope-comparable to Vietnam's localisation mandate, in scope- is extremely difficult. Indonesia provided 5 years of time for compliance, and was compelled to amend its localisation mandate due to widespread non-compliance and industry-wide lobbying (discussed in the next session)

It is important to contextualize the mandate within Vietnam's experience with Internet regulation to understand broader implications of data localisation on civil society, and its impact on the economy.

The reception of Vietnam's Cyber security law has been divided at best: 423 members of parliament, accounting for 86 percent of those present, voted in favor of the law[97], while following the vote, civil society members protested against cyber security legislations' threat to free speech[98]. Google, Facebook, and Twitter expressed concerns about the restrictive

[97] See: https://e.vnexpress.net/news/news/vietnam-says-cybersecurity-law-needed-to-ensure-national-security-3762377.html

[98] See: https://www.ft.com/content/28edfa20-6e26-11e8-92d3-6c13e5c92914

cyber security legislation, although there was no comment from either on data localisation requirements[99].

Vietnam has an active history of regulating its Internet: one of the first noted incidents of regulating the Internet came in the early 2000s, when the Vietnamese government clamped down on blogs which was deemed subversive. In 2013, it banned news reporting on social media, dictating that social media is only for personal use. 2014 in Vietnam saw the Government abuse Facebook's reporting tools to shut down dissenters, while recently it was reported that the government employed over 10,000 people to monitor Internet for dissenting voices[100].

The very nature of data localisation implies short-run costs, and a data localisation mandate with expansive scope implies higher short-run costs to the economy and a wider distribution of such costs among various stakeholders belonging to society. Estimates suggest that the overall impact of data localisation on Vietnam's economy will be negative[101], with a loss of -0.24% in Real GDP. The distribution of such costs across various sectors, and how such costs may pass on to consumers, eventually, depends on how the Vietnamese Government manages the transition into enforcing its legislated data localisation mandate.

The Vietnamese government would have to ensure infrastructural prerequisites such as uninterrupted power supply and climate controls at the cost of more productive allocation of electricity: A report by Danish Energy Agency[102] estimates that in its Business-As-Usual scenario, total final energy demand by 2035 will by nearly 2.5 times higher than in 2015. Electricity demand, the report further finds, is set to grow 8% annually until 2035, with a need to generate 93 GW power between 2015-2035. The consequent environmental costs are looming: The share of coal in total primary energy supply grew from 15% to 35% between 2000 and 2015, while biomass and hydro energy fell to 24% from 53% in the same period. An ADB assessment[103] finds CO_2 per unit of GDP rising, from its 1995 estimates to 3.39 in 2011. How costly the data localisation legislation might be will also depend on Vietnam Government's policy on how it wishes to effect a transition into the legislation: the Vietnamese Government may subsidize investments in Data center infrastructure, or enter into public-private partnership with specialized data center services, absorb costs of data center infrastructure through subsidies or other price control mechanisms etc.

Of the possible consequent benefits of installing data centers is that of gains in employment and related multiplier effects. However, the magnitude of such effects depends on the supply of skilled labor and human capital, scale and agglomeration, given the capital intensity of

99 See: https://techcrunch.com/2018/06/12/vietnams-new-cyber-security-law-draws-concern-for-restricting-free-speech/?guccounter=1

100 https://www.techdirt.com/articles/20181015/16230840845/vietnam-expands-decades-long-effort-to-crack-down-any-dissent-online-demanding-data-be-kept-country.shtml

101 Bauer et.al (2014)

102 See: https://ens.dk/sites/ens.dk/files/Globalcooperation/Official_docs/Vietnam/vietnam-energy-outlook-report-2017-eng.pdf

103 See: https://www.adb.org/sites/default/files/institutional-document/173769/vie-power-sector-reforms.pdf

such investments[104]. According to the World Economic Forum[105], Vietnam was ranked 90th in technology and innovation, and 70th in human capital, among 100 countries, rankings that reflect relative absence of readiness for Industry 4.0. Moreover, a Global Cloud Computing ranking finds Vietnam stagnating in its position (24th out of 24 countries) of preparedness for adoption and growth of cloud computing, signaling a regulatory environment not conducive for a data-driven transformation[106].

Given Vietnam's poor readiness for a data-driven Digital transformation, combined with its history of intervention in the Internet, and in some cases, in repressive ways, compliance with data localisation may mean greater State intervention in the cyber-space and potentially greater surveillance. The economic consequences will follow from Vietnam Government's ability to manage a transition towards enforcing the data localisation mandate, and trigger resurgence in readiness for digital transformation.

However, the Vietnamese government has planned a Decree on Personal Data Protection, in order to create the foundation of a unified regulation on personal data protection in Vietnam. A draft proposal, draft outline and policy impact assessment report for this upcoming decree was published by the Vietnamese government on its website on 27 December 2019.[107] It is open for public comments and opinions. Vietnam also plans to dilute its data localisation requirements under the cybersecurity law.[108]

2. Indonesia: Amending towards realistic Data Localisation

Data Localisation Legislation

Driven by rising demand for new technologies and services, Indonesia's ICT sector expanded rapidly since 2016. The number of internet users in Indonesia is projected to reach 1139.54 million users by 2022. The digital buyer penetration rate is set to grow from 9.5% in 2016 to 15.7% by 2022[109], marking a growing e-commerce market. Indonesia's Palapa Ring Broadband project is expected to connect 500 regions in the country by 2019[110], boosting the ICT capabilities of the country. In the context of a rapidly expanding digital economy, Indonesia's government deemed it necessary to regulate. In 2012, the Government legislated Government Regulation 82 that required 'Electronic System Operators' that provide 'public service' to have onshore data centers and disaster recovery centers by 15th of October 2017.

104 See: https://static.googleusercontent.com/media/www.google.com/en//about/datacenters/usstory/full-report/full-report.pdf
105 See: WEF, Readiness for the Future of Production Report (2018)
106 See: https://cloudscorecard.bsa.org/2018/pdf/BSA_2018_Global_Cloud_Scorecard.pdf
107 https://www.rouse.com/magazine/news/new-draft-decree-on-personal-data-protection-in-vietnam/
108 https://www.medianama.com/2019/10/223-data-localisation-vietnam/
109 See: Statista, Dossier on Internet Usage in Indonesia
110 See: https://www.communicindonesia.com/indonesias-ict-infrastructure-rank-second-asean-two-years-itu/

The GR82 defines:

'Electronic System Operator' as any person, state entity, business entity and community that provides, manages and/or operates an Electronic System whether independently or collectively to an Electronic System user for its own use and/or another party's use.

While the GR82 does not provide the definition of 'public services', the scope and definition of 'public services' can be found under Law No. 25 of 2009 on Public Services (Public Services Law) and Government Regulation No. 96 (GR96) of 2012 on the Implementation of the Public Services Law.

The Public Service Law defines:

'Public Services' as activities or series of activities for the purpose of fulfilling goods and services needs for every citizen and resident in accordance with the laws and regulations, and/or administrative services provided by public services providers, and treats state institutions, corporations (government owned entities), independent agencies established by law for public services activities and other legal entities established solely for public services activities

Implications and Challenges

Indonesia has had a data localisation requirement since the enactment of Government Regulation No. 82 (GR82) of 2012, with a 5-year transitional period until October 2017 for existing Electronic System Operators to comply with the regulation. However, 'Electronic System Operators' faced significant challenges in complying with the initial data localisation legislation, and have lobbied the Ministry of Communication & Information Technology (MOCI) to amend the GR82[111]. A source of difficulty in compliance stems from the GR82's ambiguity on certain key aspects of its legislation, as Baker (2017) and others have pointed out[112]: specifically, the GR82 (and GR96 for Public Services) defines 'Public Services' in a broad manner that, as a consequence, created uncertainty in practice. For instance, the broad definition of 'Public Services' allowed the MOCI to adopt an expansive interpretation and impose a registration requirement on any local Electronic Systems Operators that generally provide their services to public and/or make their services available to the public (such as social media companies, financial institutions, banking services and insurance companies etc.).

The broad ranging scope of the initial legislation posed a major challenge for business to comply and set up a data center on shore. For instance, Multipolar Technology, a listed IT company is stated to have spent $100 million to build a data center in West Java, while Google Indonesia is said to have stated to local media that regulations on data centers for

111 See: http://www.gbgindonesia.com/en/main/legal_updates/introducing_data_categorization_and_ leniency_ for _electronic_system_operators_providing_public_services.php

112 Ibid

foreign content providers are not feasible [113]. The challenge is exacerbated by the fact that it is risky and costly to establish and maintain data centers in Indonesia: the Data Center Risk rankings published by Cushman & Wakefield (2016), ranks Indonesia at 33 out of the 37 countries ranked. IDC data center index finds that the main challenge confronting Indonesian data centers is the uneven and uncertainty in distribution of electricity, exacerbated by Indonesia's distinct geographical landscape, and expanding urban spaces that demand more energy.

A research paper in 2014[114], found that costs of data localisation could be substantial for the Indonesian economy. An economy-wide data localisation measure would eliminate 12% of the country's expected economic growth in 2014 (from 5.8% to 5.1%), roughly equivalent to USD $6.1 billion, and drop Foreign Direct Investment (FDI) by 2.3%.

Such challenges and concerns from the business community compelled the MOCI to amend the GR82. The draft amendment delimits the Electronic System Operators as providing 'public service' if the electronic system operators are: 1. Regulated or monitored by sectoral agencies, 2. Provide services to Government institutions, 3. Owners of systems that are an online portal that facilitates trade, payments, and store and process personal data for operational purposes, deliver digital material through data networks, and provide communication services.

The draft amendment maintains the broad categorization of 'Public Services',and does not distinguish between public facing and non-public facing systems. However, this does not imply a sweeping data localisation mandate. The draft amendment introduced and defined three categories of data- Strategic Electronic data, High Electronic data, and Low Electronic data-that in turn determines the extent of data localisation. For instance, the draft amendment mandates data localisation for Strategic Electronic data. It allows Strategic Electronic data to be stored in the cloud, under the condition that the cloud servers are physically located in Indonesia. The same requirement is not mandated either for High or Low Electronic data. Relevant sectoral regulatory agencies are given the authority to classify data as either belonging to High or Low Electronic data, under which data can be stored and processed offshore, but must be available for supervision by the Indonesian Government.

The Indonesian Government has yet made no announcement regarding legislating on the draft amendment. However, it remains to be seen what the outcomes of the proposed data categorization would be once the amendment comes into force. While it allows companies to store data offshore, it must also ensure that strategic data is not stored in servers located outside of Indonesia. This categorization of data brought through the amendment indicates a softening of the position on data localisation and attempts to move towards a more specific set of measures to achieve the country's data protection goals.

[113] See: http://www.siia.net/blog/index/Post/67434/The-Real-World-Impacts-of-Data-Localisation-Policies
[114] See Bauer et.al (2014)

However, the government has now revoked GR 82 and introduced GR 71, with effect from October 10, 2019. Under GR 71, a new concept of public and private electronic systems operators and new and somewhat diluted data localisation measures have been introduced.[115]

3. Australia: Health Data localisation under a struggling Health Records system

Data Localisation Legislation

Digital health in Australia comprises of eHealth, hospital information systems, telemedicine, and health informatics, and deploys software, and information and communication technologies to coordinate, deliver, and manage health systems (Australian Trade Commission, 2016). Australia's health care market size in 2015 is estimated at $1.20 billion, and is expected to grow at 12.3% CAGR, between 2013 and 2020, reaching estimated market value of $2.21 billion by 2020 (Frost and Sullivan, 2015). While much of Australia's digital health initiatives are led by the private sector, Australian government's National e-Health strategy, developed in 2008, aimed to create a roadmap for several coordinated strategies to boost IT investments in Healthcare, one of which is the myHealth record, or erstwhile Personally Controlled Health Record (PCEHR) system (Australian Trade Commission, 2016).

At present, personal health record systems have not been widely used in large-scale settings, and where such large national scale systems have been deployed, such as France and UK for instance, such systems have had difficulties. The PCEHR was thought as one way to enable patient's access to health information created by them. Based on such data, the PCEHR would then target achieving a 'person-centered care' with informed customer support, improved care quality and consequently, better health outcomes for patients.

The PCEHR, which aims to serve the health care sector, is designed to be a distributed system, with multiple registered repositories in different locations marked by an Individual Health Identifier (IHI), which allows the infrastructure to collate and retrieve on request. Unlike other health banks, the infrastructure can only retrieve information sent to it from distributed repositories, using a Business-to-Business (B2B) gateway (Pearce and Bainbridge, 2014).

On the consumer side, the PCEHR is an 'opt-in' model, wherein consumers need to register to obtain an e-health record. The default mode is open access where healthcare professionals can access consumer health data, but the consumer can create a 'Restricted Access Code' (RAC) that requires healthcare professionals to obtain the RAC to access documents. Consumers can also remove or add health care providers from a list of such providers who

[115] See: https://globalcompliancenews.com/indonesia-new-regulation-electronic-systems-transactions-20191028/#:~:text=Data%20Localization%20Requirements,-There%20is%20no&text=Based%20on%20GR%2071%2C%20only,of%20Indonesia%2C%20unless%20otherwise%20regulated.

may access the record. Recently, an 'opt-out' approach was tested, wherein consumers by default have a health record, unless they 'opt-out' of the system[116].

The PCEHR infrastructure is enabled by the 'Personally Controlled Electronic Health Records Act' 2012, which defines key concepts and provisions of the PCEHR, civil penalties and, of particular importance here, the provision to investigate contraventions to the PCEHR act under the Privacy Act 1988. Under Section 77, subsection 1 provides:

The System operator, a registered repository operator, a registered portal operator or a registered contracted service provider that holds records for the purposes of the PCEHR system (whether or not the records are also held for other purposes) or has access to information relating to such records, must not: a) hold the records, or take the records, outside Australia; or b) process or handle the information relating to the records outside Australia; or c) cause or permit another person: i) to hold the records, or take the records, outside Australia; or ii) to process or handle the information relating to the records outside Australia.

Subsection 2 allows for transfer, processing, handling of data outside of Australia, provided the records don't include personal information of a consumer of the PCEHR system, or any identifying information of an individual or an entity. Chander and Le (2015) argue that under such provisions, foreign companies handling health-related information must build data centers or outsource such operations to local services in Australia.

Implications and Challenges

Data localisation in Australia is mandated through the My Health Records Act (erstwhile, Personally Controlled Health Records Act), and applies to data held under My Health Records system. The health records system falls under public health care, with the Secretary of the Department of Health responsible for the data and operations of the health records system.

With respect to Data Localisation, the experience of the My Health Record System demonstrates data localisation laws' inability to induce additional confidence and trust to support the health records system. As will be described below, the receding legitimacy of Australian health record system, and non-restrictive cloud data transfer provisions undermines the need for data localisation.

The health record system has been experiencing critical challenges that appear to question the legitimacy of its existence. Firstly, the health record system is facing crisis of viability [117]: The My Health Record compulsorily enlists all Australians into sharing their health information. But when the Australian government made available the option of opting out of the health records system, the number of opt-outs, which also involves the 'right to be

[116] See: https://www.myhealthrecord.gov.au/for-you-your-family/opt-out-my-health-record

[117] See: https://www.aei.org/publication/data-privacy-debacle-down-under-is-australias-my-health-record-doomed/

forgotten' were so large that the Australian Digital Health Agency (ADHA), which runs the My Health Record system was telling callers they didn't expect the volume of opt outs[118]. The sheer weight of applications for opting out caused ADHA systems to crash. $114 million in funds were provided for informing the public about the opt-out, including A$27.75 million to develop collateral and support, A$52.38 million for training healthcare providers and A$34 million for the call center. A total of A$4 billion was spent to date on the health records system that is currently facing such severe backlash.

Then there is the crisis of credibility: the design of the My Health Records system is similar to England's care.data, which collapsed for failing to bring along the public, and which was subject to series of damning independent reviews.[119] Poor adoption rates during My Health Record's test run forced the Australian Government to make it an opt-out system[120]. Given that all Australians are automatically enlisted, and must create passwords to safeguard personal data, the health record, by design, does not regard individual consent. A media investigation also revealed that apps have been accessing sensitive personal information from My Health Records to pass on to personal injury lawyers seeking clients for injury claims[121]. Reports that data on My Health Records was used to track down fleeing mother and child from violent households further dents the claim that the health record system gives any regard to individual privacy and security[122].

Data localisation mandate applies only to the My Health Records data, which is only a part of the total data that public and private healthcare entities collect. This weakens the case for the localisation of My Health Records.[123] Moreover, the data localisation mandate does not seem to improve either the crisis of legitimacy or the crisis of credibility facing Australia's healthcare industry. The situation is worsened by the fact that the healthcare sector is increasingly vulnerable to data breaches[124], further undermining the case for data localisation of health records, in Australia.

4. South Korea: Spatial Data Localisation for National Security

Data Localisation legislation

The case of South Korea's spatial and location information data localisation is distinct because it was not so much a reaction to the Snowden allegations as it is a result of its war with North Korea. The Data localisation measures were in place since the ceasefire with North Korea in the 1960s. South Korea legislated two data localisation laws:

---

118 See: https://www.zdnet.com/article/my-health-record-systems-collapse-under-more-opt-outs-than-expected/

119 See: https://www.theguardian.com/technology/2016/jul/06/nhs-to-scrap-single-database-of-patients-medical-details

120 See: https://www.aei.org/publication/data-privacy-debacle-down-under-is-australias-my-health-record-doomed/

121 See: http://www.abc.net.au/news/2018-06-25/healthengine-sharing-patients-information-with-lawyers/9894114

122 See: https://indaily.com.au/opinion/2018/09/21/doubts-remain-about-the-safety-of-my-health-record/

123 See: https://www.microsoft.com/en-sg/apac/trustedcloud/australia-healthcare-service.aspx

124 See: https://www.smh.com.au/technology/australians-are-rightly-questioning-my-health-record-says-privacy-commissioner-20180730-p4zui3.html

1. The Korean Spatial Data Protection Act

Korean Spatial Data protection Act: The origin of the Act on the establishment, management etc., of spatial data has its origins in the 1961 Land Survey Act, which was legislated to prevent hostile entities from obtaining maps of the country[125]. Article 16 provides for:

16 (1). No person shall take abroad maps, etc. or photos produced for the purpose of survey among the results of a fundamental survey without permission of the Minister of Land, Infrastructure, and Transport.

16(2). No person shall take abroad the results of a fundamental survey in cases of falling under any subparagraph of Article 14(3), where it is likely to harm national security or other important national interests.

2. The erstwhile Regulation on Supervision of Credit-Specialized Financial Business

Under this regulation, e-commerce firms selling goods in Korean won have been prohibited from storing Korean customer's credit card numbers in company information systems. U.S. e-commerce firms for instance, continue to sell legally into Korean markets from abroad, setting prices in dollars, but are prevented from accepting Korean-branded credit cards.[126] There are two other important legislations that govern data protection, but which do not mandate data localisation:

1. *Personal Information Protection Act (PIPA, 2011):*

PIPA regulates the collection, use, provision, outsourcing, storage and obstruction of personal information including user's names, addresses, photographs etc.[127] PIPA includes regulation for data exports, and this is covered in the article 17(3) of the Act:

'When a personal information manager provides a third person at any overseas location with personal information, he/she shall notify a subject of information of the matters referred to in each sub paragraph of paragraph (2) and obtain consent thereto, and shall not enter into a contract concerning the trans-border transfer of personal information stipulating any details contravening this Act[128].

2. *Act on the Protection of Location Information:*

Article 15 of the act stipulates that collection, use, or providing of an individual or mobile object without the consent of that individual or the owner of the object is prohibited[129]. Thus, under this law, a person's and person owned object's location information is subject to data protection.

---

125 See: Chander and Le (2014)
126 See: USTR (2017)
127 See: http://koreanlii.or.kr/w/images/0/0e/KoreanDPAct2011.pdf
128 Ibid
129 See: http://elaw.klri.re.kr/kor_service/lawView.do?hseq=33741&lang=ENG

Implications and Challenges

Broadly, the set of legislations, which constitute a part of South Korea's Data protection regime as mentioned in the previous section, affect two classes of economic activities: 1. Performance of location-based services, 2. Performance of maps-based Apps.

The location-based services are services based on geographic information provided by wired/wireless communication networks. These include service such as location tracking, location 'check-in' on mobile phones that use GPS, among others.

The Spatial Data protection combined with Personal Information Protection Act and the Act on the Protection of Location Information effectively regulate data flows in the location-based services industry. Data from Korea Communications Commission shows that the market for location-based services has been growing with the rapidly expanding mobile phone market, since 2010. In 2016, there were 180 registered location information providers and 936 location-based service providers. An analysis of the categories of services provided by the industry shows that marketing and business transactions accounted 35.1% or 296.1 billion won, lifestyle and entertainment accounted for 13.8% or 114.3 billion won, and management operations 12.4% or 102.6 billion won, with the industry in total generating 1.2 trillion won in revenues, in 2017.[130]

Growth in the market for location-based services is skewed towards medium and large scale firms however: small businesses account for more than half of the market for location based services but capture only 19.5% of the profits generated by the industry[131]. Moreover, the industry may not have reached full potential: The KISA (2017) finds that the legislations have been criticized claiming they impede promotion of location-based services, are outdated and do not protect personal security. Its survey[132] of 224 location-based services companies approved by the Korea Communications Commission and found that 35.7% of participants saw regulatory measures as the biggest to the growth of the location-based services market and stated that deregulation and eased standards for location information protection could serve as important market boosters. The future of the market for location-based services may compel a regulatory review, as the proliferation of IoT will act as a major driver of growth in the industry.

The Spatial Data protection act initially targeted physical materials when it was first enacted but now has been expanded to digital data, prohibiting foreign companies from using South Korean map resources, unless it meets the localisation requirement as stated in the previous section. In 2016, Google requested permission to use government mapping data in servers outside the country citing the need to use data on servers worldwide to enable services that would give walking and driving directions in South Korea. The South Korean court determined that the security risks of providing the data to Google outweighed the convenience of the company's Maps services. The ruling means that the app can't offer

130 See: http://koreabizwire.com/revenue-from-location-based-services-to-grow-by-25-pct-this-year/111254
131 See: http://koreabizwire.com/south-korean-location-based-services-market-growing-rapidly/82507
132 Ibid

walking or driving directions in South Korea, but the negative impacts can be potentially offset by South Korea's fast and cheap Internet access, and online navigation, which however, is only available through local companies, in Korean.[133] The Government, in 2016 however offered access to map data under the condition that Google reduce map resolutions for important landmarks such as military outposts and government offices. The court case was a result of Google's refusal to comply with this alternative[134].

The Spatial Data protection has also acted as a protectionist barrier to foreign competition and enabled indigenous companies such as Naver and Kakao to locally compete with giants such as Google. Although, Google beat Naver in monthly users of mobile maps in April, 2018- Google Maps had 8.32 million users in April, 2018, above the 7.77 million posted by Naver Map- Google's global stronghold over its search engine popularity finds an outlier in South Korea, with Naver's search engine providing close competition: A Statista Global Consumer Survey found that 92% of respondents said they used Naver's search engine when asked which search engines they have used in the past 4 weeks. Google received 65% of the responses[135]. A ranking of the most popular online properties in South Korea as of May, 2018, by number of visitors shows Naver online portal website ranking first with 29.06 million unique visitors, with Google ranking 5th with 13.17 unique visitors.

South Korea's data localisation may be considered to have enjoyed relative success over other cases reviewed here, presumably because the circumstances under which the data localisation measure was legislated were exceptional and demanded strict enforcement. Further, the data localisation measure is very specific, and restricted only to a particular class of sensitive and high value data. However, the proliferation of IoT and new technologies that leverage location-based data will strain strict data localisation of location-based data, and will require regulatory innovations on part of South Korea.

133 See: https://www.csmonitor.com/Technology/2016/1118/Why-South-Korea-refuses-to-share-mapping-data-with-Google

134 See: https://nationalinterest.org/blog/the-buzz/one-thing-north-korea-has-the-south-doesnt-google-maps-24650

135 See: https://www.statista.com/forecasts/826419/popular-search-engines-in-south-korea

Indian Council for Research on International Economic Relations (ICRIER)
4th Floor, Core 6A, India Habitat Centre, Lodhi Road, New Delhi-110003