GEGAFRICA
GLOBAL ECONOMIC GOVERNANCE

DISCUSSION PAPER | APRIL 2018

SOUTH AFRICA AND DATA FLOWS

HOW TO FULLY EXPLOIT THE POTENTIAL OF THE DIGITAL ECONOMY

Martina F Ferracane

GEGAFRICA
GLOBAL ECONOMIC GOVERNANCE

ABOUT GEGAFRICA

The Global Economic Governance (GEG) Africa programme is a policy research and stakeholder engagement programme aimed at strengthening the influence of African coalitions at global economic governance forums such as the G20, BRICS, World Trade Organization and World Bank, among others, in order to bring about pro-poor policy outcomes.

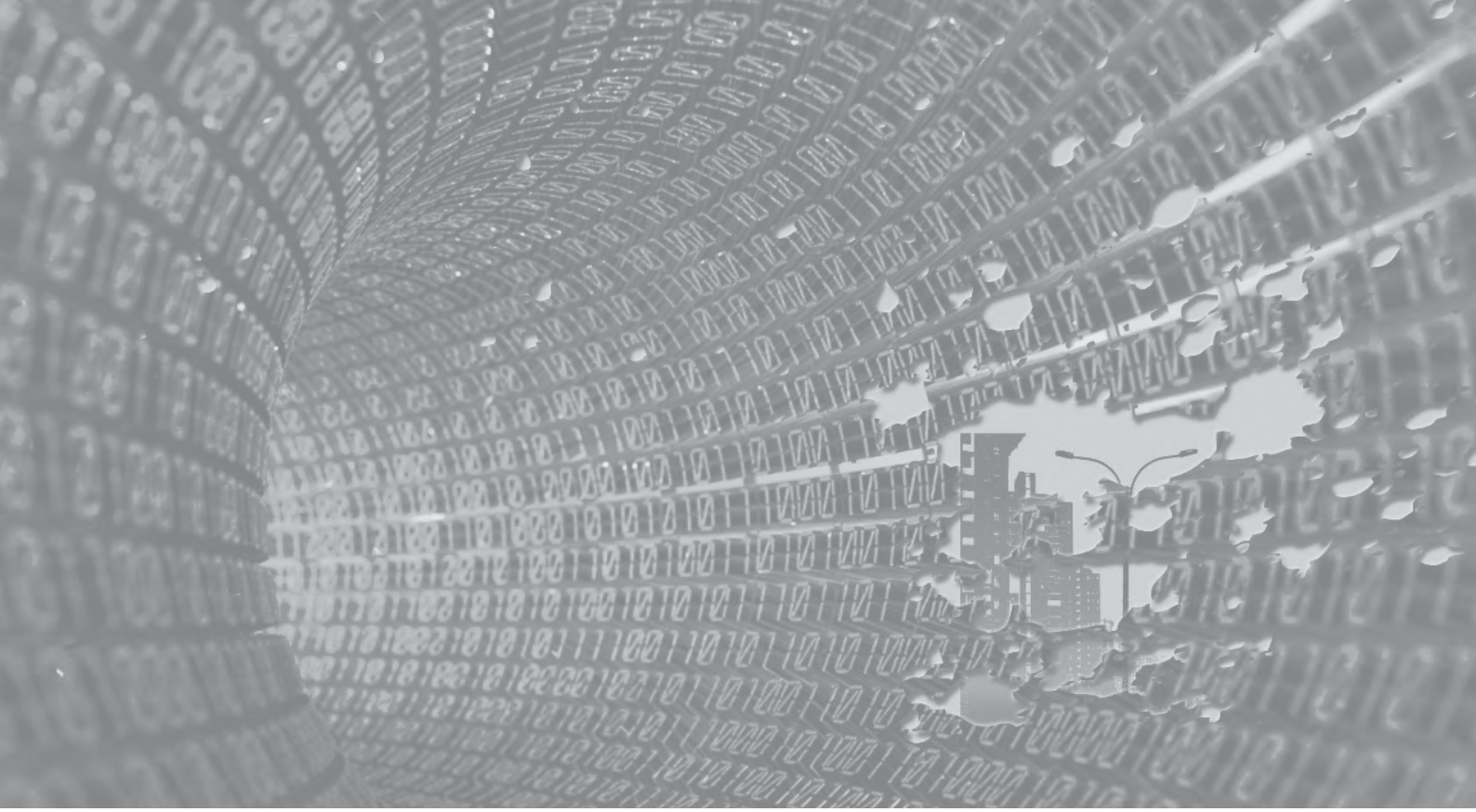
The second phase of the programme started in March 2016 and will be implemented over a period of three years until March 2019.

The programme is expected to help create an international system of global economic governance that works better for the poor in Africa through:

- undertaking substantial research into critical policy areas and helping South African policymakers to prepare policy papers for the South African government to present at global economic governance platforms;
- ensuring that African views are considered, knowledge is shared and a shared perspective is developed through systematic engagement with African governments, regional organisations, think tanks, academic institutions, business organisations and civil society forums; and
- disseminating and communicating research and policy briefs to a wider audience via mass media and digital channels in order to create an informed and active policy community on the continent.

The programme will be focused on three thematic areas: development finance for infrastructure; trade and regional integration; and tax and transparency.

GEGAFRICA is funded by the UK Department for International Development and managed by a consortium consisting of DNA Economics, the South African Institute of International Affairs and Tutwa Consulting.



DISCUSSION PAPER
APRIL 2018

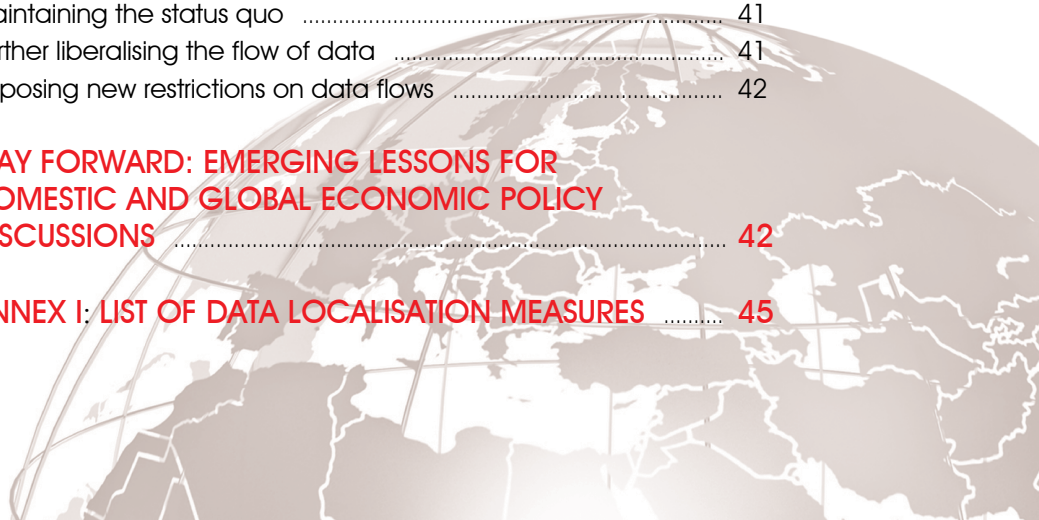
SOUTH AFRICA AND DATA FLOWS

HOW TO FULLY EXPLOIT THE POTENTIAL OF THE DIGITAL ECONOMY

Martina F Ferracane

GEGAFRICA
GLOBAL ECONOMIC GOVERNANCE

CONTENTS

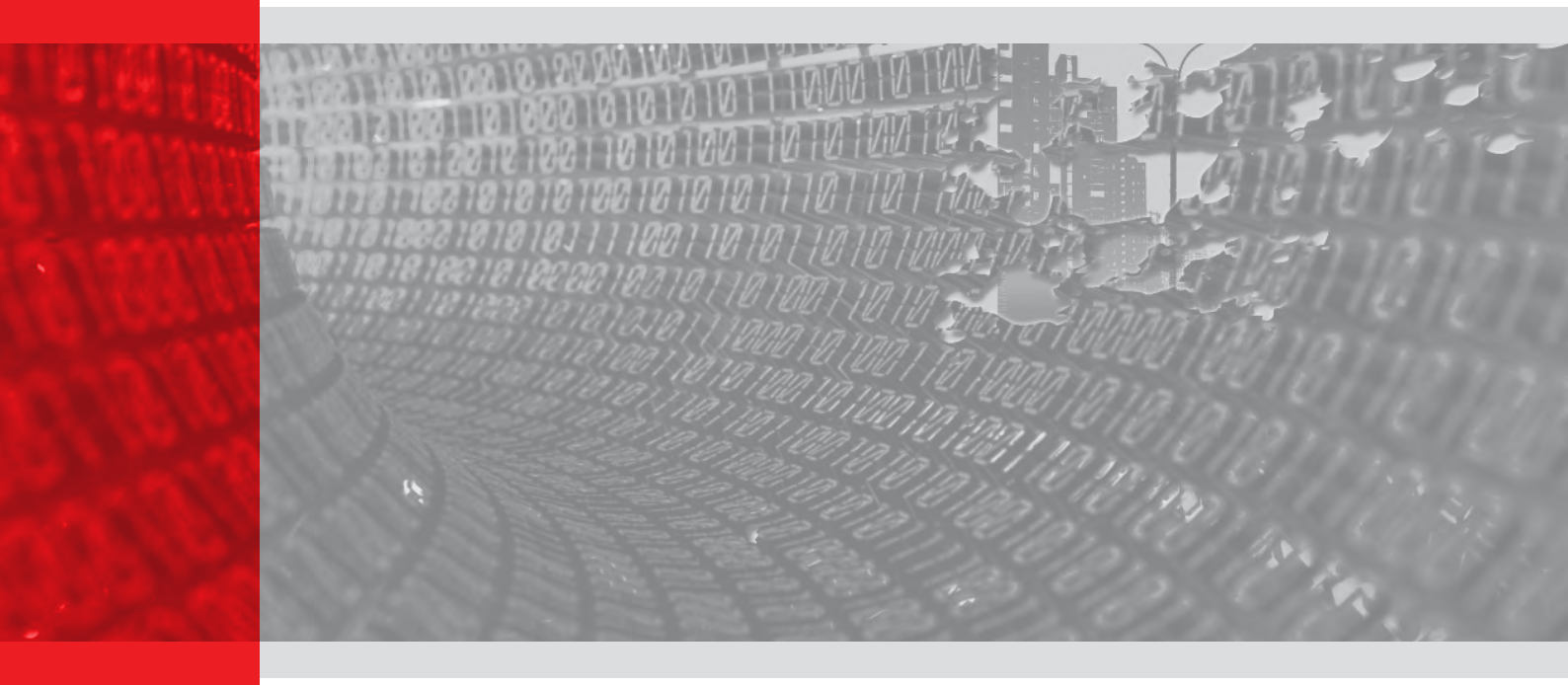


ABSTRACT

South Africa is in a privileged position to become the regional hub for provision of data processing services and other innovative digital services. In order to do so, the country should promote the free flow of data, allowing local companies to extract the benefits of data created regionally. This paper provides clear economic arguments to support such a regime in South Africa, and shows that restrictions on movement of data have detrimental effects on productivity, innovation, access to information, investment and ultimately the growth and welfare of the country. The introduction of this paper looks at the importance of data in today's digital economy, while section two introduces the issue of restrictions to data flows, and clarifies the current state of play when it comes to such restrictions, both globally and in BRICS countries. The third section discusses data policy regimes in BRICS economies. Section four provides a broad analysis of the costs of data flow restrictions for countries implementing these policies. Section five summarises how data flows are regulated in free trade agreements, and provides food for thought on a multilateral discussion on the issue. Section six shows the options ahead for South Africa, and the paper concludes with recommendations for South Africa on how to fully exploit the benefits of the digital economy.

AUTHOR

Martina F Ferracane is a PhD student in Law and Economics at Hamburg University and a Research Associate at ECIPE (European Centre for International Political Economy), researching digital trade issues and data flows. She also founded and is currently managing FabLab Western Sicily, a non-profit organisation that is bringing digital fabrication to Sicilian schools. She is passionate about digital entrepreneurship and recently co-founded Oral3D, a start-up in the area of 3D printing and dentistry. Previously, she worked at the European Commission and the UN.



INTRODUCTION

Movement of data across borders is central to today's economy: it enables people to instantly connect with each other, companies to do business smoothly and governments to offer new, more efficient services to their citizens. The Internet has fundamentally changed with whom, what and how trade is conducted, and today virtually all cross-border transactions make use of the Internet or some digital component.

Online access and the ease of online communication has been one of the driving forces behind the consolidation of global value chains, the participation of small and medium enterprises in global trade, and an increase in economic activity in developing economies.[1] Data flows are creating significant value for the global economy and exert a greater impact on growth than traditional goods flows.[2]

Firms rely on data for all sorts of activities: research and development, human resource management, the coordination of production processes and supply chain

1 Baldwin R, *The Great Convergence: Information Technology and the New Globalization*. Cambridge: Belknap Press, 2017.

2 McKinsey estimates that data flows have contributed about $2.8 trillion to the global economy in 2014 alone. McKinsey Global Institute, *Digital Globalization: The New Era of Global Flows*, McKinsey & Company, March 2016.

management, in-plant production, and sales and post-sales;[3] and the exponential growth in data being exchanged cross-border is not set to slow down.[4] Yet today most data processing and data-intensive activities remain in the hands of a few companies.

Despite these significant benefits, the concentration of these activities in the hands of certain multinationals has raised the question of whether countries should insist that companies process their citizens' data within their jurisdictions. Intuitively, keeping data locally seems to be the best option to fully exploit its potential and ensure that the country gets a share of the profits created by these companies.

This paper explores this phenomenon and clarifies why this perception is often mistaken. Restrictions to data flows – often referred to as data localisation measures – are detrimental to the local economy, and impose unnecessary costs on local businesses and consumers. In fact, keeping data within the country does not automatically translate into greater value for local companies.

Without the ability to exploit data, the economy will not benefit from it. Local companies today use foreign data processing services to harvest safely and efficiently the data created in their economy. Without this option, most developing countries risk missing the opportunity to fully exploit the potential of the digital economy.

The second section of this paper provides an introduction to data flows and the different regulatory regimes that restrict the flow of data, as well as an analysis of the sectors and types of data affected. The third section summarises the policy regime in the BRICS economies, while the fourth section focuses on the cost of data localisation and presents a literature review of studies that attempt to estimate the economic cost of restricting movement of data cross-border. The following section summarises the current policy discussion on data flows in trade agreements and other relevant initiatives. This is followed by possible regulatory options for South Africa when it comes to data flows, while the paper concludes with some remarks and emerging lessons for domestic and global economic policy discussions.

DATA FLOWS: REGULATORY REGIMES APPLIED WORLDWIDE

Regulation of data flows has become a hot topic in policy debate given the modern economy's increasing reliance on data flows. Certain countries have not imposed any restrictions on the movement of data across borders, while others have responded by restricting movement of certain (or even all) data in their jurisdiction.

3 Swedish National Board of Trade, 'No Transfer, No Production – A Report on Cross-Border Data Transfers, Global Value Chains, and the Production of Goods'. Stockholm: Kommerskollegium, 2015.

4 McKinsey Global Institute, *op. cit.*

Cross-border movement of data can be restricted by different types of measures, which can also target specific sectors or types of data. This section provides an overview of the different regulatory regimes applied globally. The analysis is based on a dataset of policy measures in 64 major economies worldwide, retrieved from the Digital Trade Estimates (DTE) database developed by the European Centre for International Political Economy (ECIPE).[5]

Types of restrictions on movement of data

Current restrictions on data flows are either measures that pre-date the Internet and that have resulted in restrictions in the online world, or the response of certain governments to concerns about the digital economy. Examples of measures pre-dating the Internet that now restrict data flows are policies requiring the local storage of business accounting data, which are still in place in certain European countries.[6] These policies were designed to ensure that the government had easy access to accounting data in case of an audit. In the 1980s, this was the only way to ensure that the data could be provided swiftly to the public authorities. However, in the Internet era this requirement has become obsolete, and adds unnecessary costs for companies without actually facilitating access to such data. It is not surprising therefore that they are now being lifted by several governments.

There are five degrees of restrictions on movement of data across borders. Figure 1 ranks the regimes from least to most restrictive in terms of the ease with which companies can move data across borders.[7]

The first, and least restrictive, regime is when the country does not impose any restrictions on data movement. This means that data can be stored and processed in any country, and the company decides where data is located. This regime facilitates cross-border data flows, and in particular the use of cloud computing solutions.

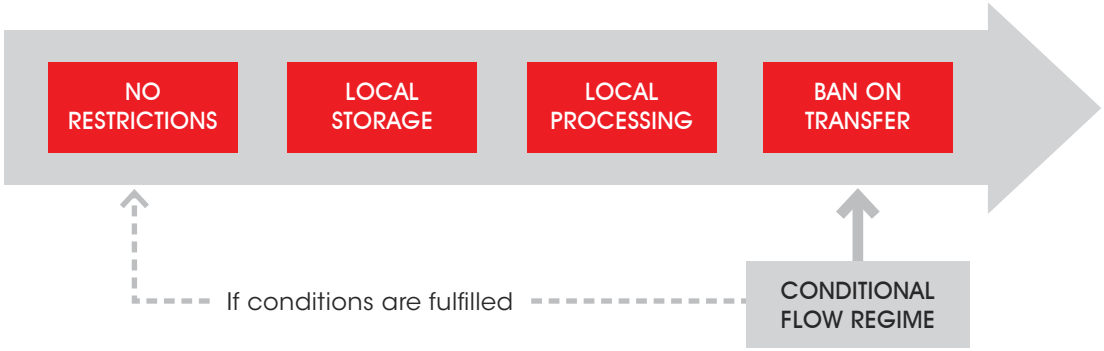
The second degree is when a country imposes a local storage requirement, where companies are required to store a copy of certain data within the country: the data can still be transferred and processed abroad. As long as a copy of the data remains within the national territory, the company can operate as usual. Local storage requirements often apply to specific data such as accounting or bookkeeping data.

5 In addition to the 28 member states of the EU, the analysis also covers the following countries: Argentina, Australia, Canada, Chile, China, Colombia, Costa Rica, Ecuador, Hong Kong, Iceland, India, Indonesia, Israel, Japan, Malaysia, Mexico, New Zealand, Nigeria, Norway, Pakistan, Panama, Paraguay, Peru, Philippines, the Republic of Korea, the Russian Federation, Singapore, South Africa, Switzerland, Taiwan, Thailand, Turkey, the US and Vietnam.

6 Borgreen C, 'New Research: Conflicting Company Data Rules Inhibit Intra-EU Business', Disruptive Competition Project, 23 February 2016, http://www.project-disco.org/information-flow/022316-new-research-conflicting-european-accounting-rules-inhibit-intra-eu-business/#.WXctT9OGOu4, accessed 23 August 2017.

7 Countries can apply different types of restrictions to different sectors and types of data; therefore one country may have several restriction levels.

FIGURE 1 TYPE OF RESTRICTIONS ON CROSS-BORDER MOVEMENT OF DATA



Source: Ferracane MF, 'Restrictions to Cross-Border Data Flows: a Taxonomy', ECIPE Working Paper, 1, November 2017

The third degree is the case of local storing and processing. When a country imposes this requirement, companies have to store and process data within the country. This means that companies need to use data centres located in the country for the main processing of data, and must therefore either build a data centre or switch to local providers of data processing solutions. Alternatively, certain companies might decide to leave the market altogether. If this regime applies, a copy of the data can still be sent abroad, for example to the parent company. This requirement has recently been introduced in Russia, with the amendment of the Russian Data Protection Law by Federal Law No. 242-FZ in July 2014.[8] Article 18 §5 requires data operators to ensure that the recording, systematisation, accumulation, storage, update/amendment and retrieval of personal data of citizens of the Russian Federation are made using databases located in the Russian Federation.

The fourth, and most restrictive, degree is a ban on transfers of data abroad. When this requirement applies, the company cannot transfer certain data abroad. Such a policy usually applies to specific sets of data considered especially sensitive, such as health or financial data. The difference between a ban on transfers and a local processing requirement is quite subtle. In the first case, the company is not allowed to send even a copy of the data cross-border. In the second case, the company can still send a copy of the data abroad, which can be important for communication between a subsidiary and its parent company, and in general for exchanging information within the company. In both cases, however, the main data-processing activities need to be done in the country. To date, no country has imposed a ban on the transfer of *all* data abroad. Yet several countries impose this restriction on

8 This amendment entered into force on 1 September 2015.

specific sets of data. China, for example, bans the transfer abroad of financial and health data.[9]

The fifth category is the conditional flow regime, where the transfer of data abroad is forbidden unless certain conditions are fulfilled. The conditions can apply either to the recipient country (eg, some jurisdictions require that data be transferred only to countries with an 'adequate' level of protection) or to the company (eg, a common condition is that the data subject must consent to the cross-border transfer of his/her data). When the conditions are met, the data can flow freely. However, if the conditions are stringent, the measure can easily result in a ban on transfers.[10]

The most common example of a conditional flow regime is the European regime of data protection, which has inspired many other countries to implement similar policies, including South Africa. The regime is undergoing an update with the replacement of Directive 95/46/EC, in place since 1995, with the General Data Protection Regulation (GDPR), which will enter into force in May 2018.[11] According to the current regime, data is freely allowed to flow outside the European Economic Area (EEA) only where:

- the recipient jurisdiction has an adequate level of data protection;[12]
- the controller adduces adequate safeguards (for instance, by using model contract clauses, binding corporate rules or other contractual arrangements);
- the data subject has given his/her unambiguous consent;
- the transfer is necessary for the performance of a contract between the data subject and the controller;

9 In terms of financial data, according to the 'Notice to Urge Banking Financial Institutions to Protect Personal Financial Information', the processing of personal information collected by commercial banks must be stored, handled and analysed within the territory of China and such personal information may not be transferred overseas. In relation to health data, 'China's Management Measures for Population Health Information' require that citizens' health information is stored and processed within China. In addition, storage is not allowed overseas. For more information, see Thomson Reuters Practical Law, 'Data protection in China: Overview', 2016, http://uk.practicallaw.com/4-519-9017, accessed 17 August 2017.

10 In certain cases it is not easy to discern whether a measure is a ban on transfers, a local processing requirement or a conditional flow regime. In fact, transfer bans and local processing requirements often have certain exceptions that might *de facto* result in a conditional flow regime.

11 The conditions for the transfer of data abroad have remained roughly unchanged despite a tightening of certain conditions. The text of the GDPR is available at European Commission, 'Data protection', http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf, accessed 31 August 2017.

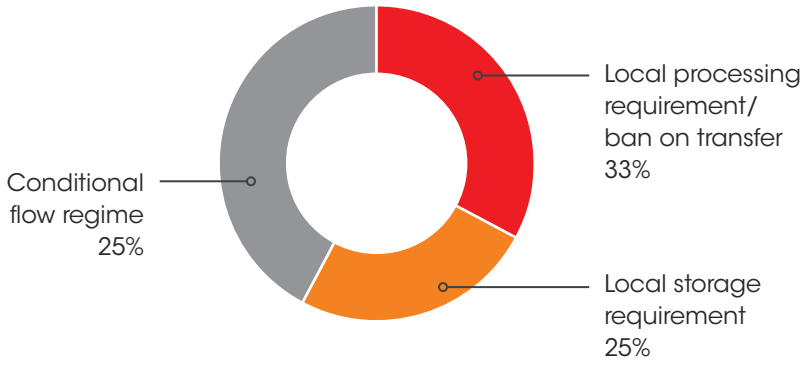
12 At the time of writing, 12 jurisdictions had been deemed to have an adequate level of protection: Andorra, Argentina, Canada, Faroe Islands, Guernsey, Jersey, the Isle of Man, Israel, New Zealand, Switzerland and Uruguay. In addition, the EU/US Safe Harbour acted as a self-certification system open to certain US companies for data protection compliance, until its invalidation by the European Court of Justice in October 2015. The system was replaced by the Privacy Shield in July 2016.

- the transfer is necessary for the performance of a contract concluded in the interest of the data subject;
- the transfer is justified by public interest;
- the transfer is necessary to protect the vital interests of the data subject; and/or
- the data is public.

To summarise, countries that impose restrictions on movement of data do so by requiring that a copy of the data be stored and/or processed locally, by banning the transfer of data abroad, or by imposing certain conditions on the transfer abroad. Measures restricting the flow of data are usually referred to as data localisation measures, as they create incentives for data to be localised in a certain jurisdiction.[13] According to ECIPE's analysis of 64 countries, 87 data localisation measures are currently in force.[14]

Most of these measures impose a conditional flow regime (42%), with stricter restrictions on data processing and transfer bans covering about a third of the measures (see Figure 2).[15] Finally, local storage requirements are found in 25% of the total cases in which certain restrictions are imposed.

FIGURE 2 TYPE OF DATA LOCALISATION MEASURE IMPOSED



Source: Own calculations based on data retrieved from ECIPE Digital Trade Estimates (DTE), database, www.ecipe.org/dte/database, accessed 17 August 2017

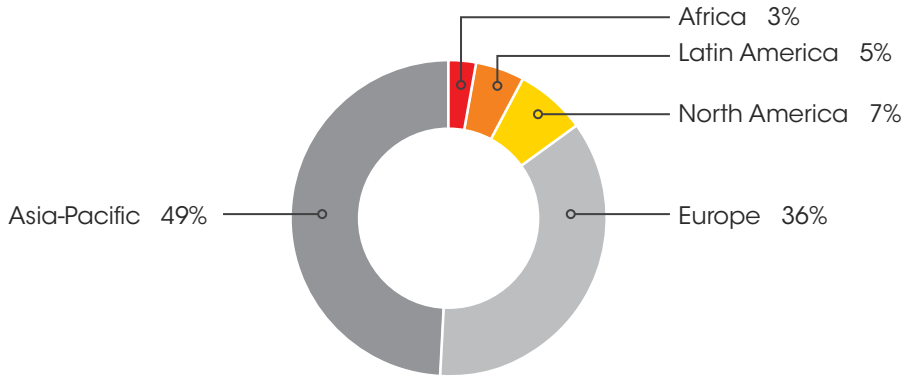
13 Certain studies also use the term 'data residency' requirement.

14 ECIPE (European Centre for International Political Economy) Digital Trade Estimates (DTE), database, www.ecipe.org/dte/database, accessed 17 August 2017. The complete list of the measures can be found in Annex I.

15 As mentioned above, local processing requirements and bans on data transfers have a similar impact on businesses and are not always easy to differentiate from one another. Therefore, they are grouped in a single category for the purpose of this analysis.

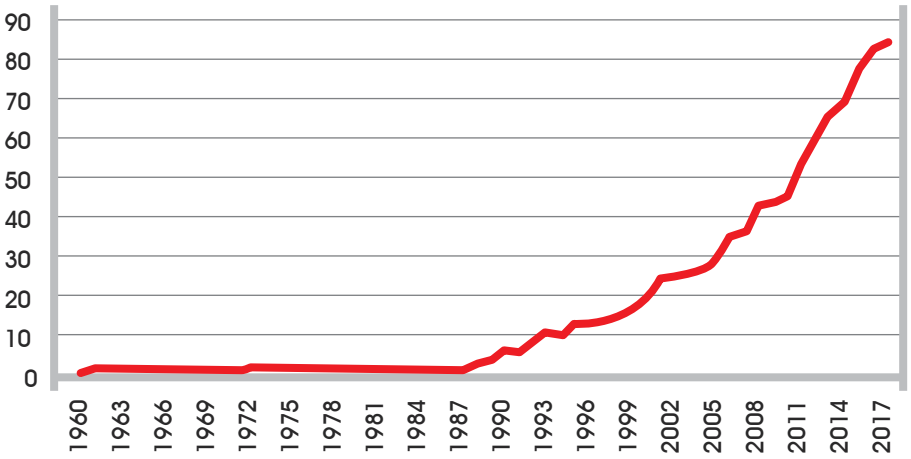
About half of the measures found are imposed by Asian countries (Figure 3), while Europe and Asia-Pacific together account for 85% of all measures collected and the BRICS countries for about 20% – most of which are implemented in China and Russia.

FIGURE 3 GEOGRAPHICAL COVERAGE OF DATA LOCALISATION MEASURES[16]



Source: Own calculations based on data retrieved from ECIPE DTE, database, http://www.ecipe.org/dte/database, accessed 17 August 2017

FIGURE 4 CUMULATIVE NUMBER OF DATA LOCALISATION MEASURES (1960–2017)



Source: Own calculations based on data retrieved from ECIPE DTE, database, www.ecipe.org/dte/database, accessed 17 August 2017

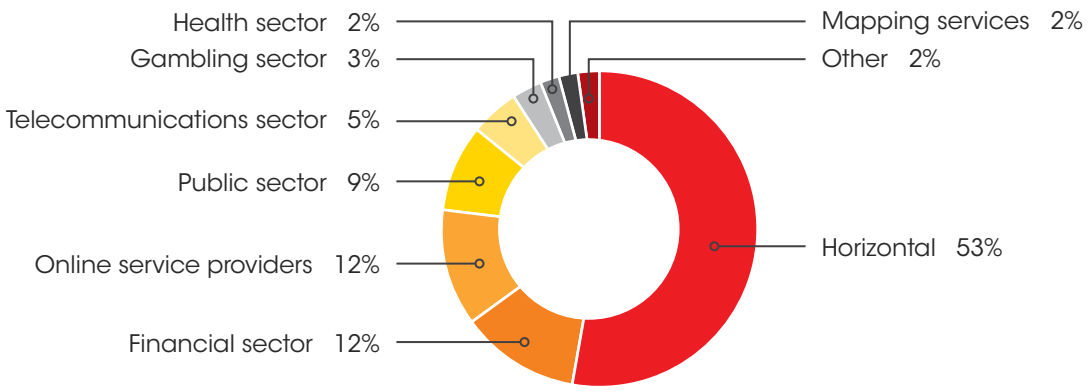
16 The Russian Federation is listed under the 'Asia-Pacific' region.

As shown in Figure 4, the last decade has seen a worrying rise in data localisation measures being implemented worldwide. The oldest measure, which actually pre-dates the Internet but was later also enforced online, was implemented in as early as 1961. Until 2000 only 20 measures were imposed globally. However, by 2008 the number of measures more than doubled, and doubled again by 2017.

Types of sectors affected by restrictions

While most of the measures are horizontal and therefore apply to all sectors (53%), about half are sector-specific. These measures target in particular online service providers,[17] the financial, public, telecommunications, gambling and healthcare sectors, and mapping services (Figure 5). The data shows that bans on the transfer of data and local storage requirements tend to be sector-specific, while conditional flow regimes tend to be horizontal as they apply mostly to personal data in all sectors.

FIGURE 5 SECTORAL COVERAGE OF DATA LOCATIONAL MEASURES



Source: Own calculations based on data retrieved from ECIPE DTE, database, www.ecipe.org/dte/database, accessed 17 August 2017

Types of data affected by restrictions

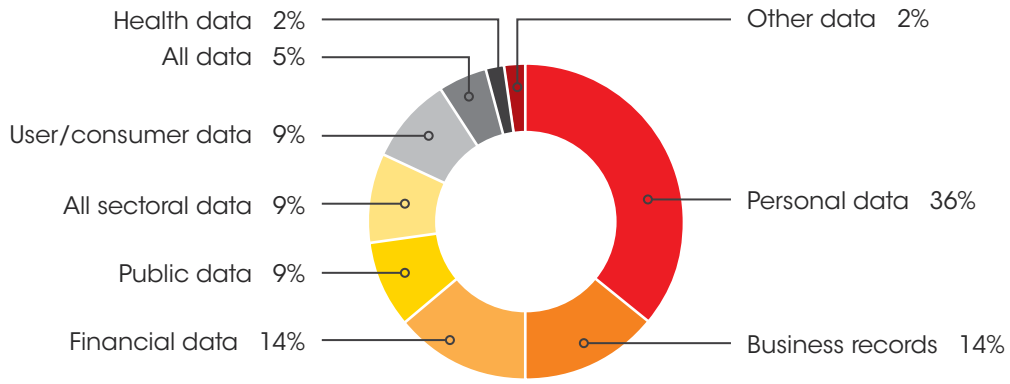
More than a third of all measures identified apply to personal data (Figure 6). As mentioned above, they often relate to conditional flow regimes that apply horizontally to all sectors. Given the increasing technical difficulties and costs

17 This category covers several definitions provided by countries to cover different sets of operators online. Depending on the country, companies under this definition range from advertising companies to cloud providers.

encountered in separating personal from non-personal data (especially with new advances in the realm of the Internet of Things), in the near future measures that apply to personal data are likely to apply *de facto* to all data in the economy.

In addition, 14% of measures apply to business records. In these cases, the measures applied are usually local storage requirements, implemented to facilitate access to such data by governments when this data is needed swiftly. Other types of data targeted are financial data (14% of measures), followed by public data, user data and all data in a certain sector (9% in each case). A few measures (5%) apply to all data in the economy, and 2% of measures apply to the healthcare sector.

FIGURE 6 TYPE OF DATA TARGETED BY DATA LOCALISATION MEASURES



Source: Own calculations based on data retrieved from ECIPE DTE, database, www.ecipe.org/dte/database, accessed 17 August 2017

DATA FLOW REGIMES IN THE BRICS ECONOMIES

The BRICS economies have responded differently to the Internet revolution, although they all implement or plan to implement certain restrictions on data flows. China and Russia impose the strictest regimes – not only among the BRICS countries but also globally.[18] These countries see the Internet as a crucial offensive interest in international geopolitics, and have therefore prioritised public order and security concerns over economic ones.

Brazil and India, on the other hand, initially considered imposing strict restrictions as a means to promote national industries, but ultimately opted against such measures.[19] This is probably owing to the consideration that short-term gains from

18 Ferracane MF & E Van der Marel, 'Digital Trade Restrictiveness Index, ECIPE (forthcoming).

19 As presented in detail below, India does impose certain restrictions in the public sector.

restricting data flows would be offset by losses in productivity, investment and ultimately growth.[20]

To date South Africa has neither imposed nor considered imposing strict restrictions, although the country has a conditional flow regime in place.

China and Russia see the Internet as a crucial offensive interest in international geopolitics, and have therefore prioritised public order and security concerns over economic ones

This section summarises the regulatory regime applied in South Africa, and compares it to the regime implemented by the other BRICS countries.

South Africa

South Africa does not impose strict restrictions on data transfers. Yet the country has implemented certain restrictions through a conditional flow regime that takes inspiration from the European model. According to the Protection of Personal Information (POPI) Act 4 of 2013, data can be transferred to third countries only when:

- the recipient is subject to a law, binding corporate rules or a binding agreement that:
  - » upholds principles for reasonable processing of information that are substantially similar to the conditions contained in POPI; and
  - » includes provisions that are substantially similar to those contained in POPI relating to the further transfer of personal information from the recipient to third parties who are in another country;
- the data subject consents to the transfer;
- the transfer is necessary for the performance of a contract between the data subject and responsible party, or for the implementation of pre-contractual measures taken in response to the data subject's request; and/or
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the responsible party and a third party, or the transfer is for the benefit of the data subject and:
  - » it is not reasonably practicable to obtain the consent of the data subject to that transfer, and
  - » if it were reasonably practicable to obtain such consent, the data subject would be likely to give it.

20 The economic implications of data flow restrictions are discussed in detail in the section on the cost of data localisation.

Besides the conditional flow regime, South Africa does not impose any local storage and processing requirements. Therefore, despite the presence of certain restrictions, South Africa's regime is in line with that of India and the proposed regime in Brazil, and is significantly less restricted than those of China and Russia.

South Africa's regime is in line with that of India and the proposed regime in Brazil, and is significantly less restricted than those of China and Russia

Brazil

Brazil does not have a single statute establishing a data protection framework. The Data Protection Bill is before Congress and, when enacted, will specifically and broadly regulate such subject matter. The bill is currently being reviewed by the House of Deputies, where it is expected to be analysed by three commissions: the Commission of the Constitution, Justice and Citizenship; the Commission of Science, Technology, Communication and Informatics; and the Commission of Labour and Public Administration. Public consultations and open debate are expected to take place following the bill's approval by the three commissions. While the procedural protocol for this bill has been tagged as urgent, it is not possible, at this moment, to say when the vote will take place.[21]

The bill has an entire chapter dedicated to international transfers. Article 33 of the bill establishes that an international transfer will only be allowed if provided to countries with equivalent levels of data protection or when expressly consented to by data subjects, after specific information concerning the international nature of the operation and the risks entailed has been given. The bill also contains a limited number of exceptions, and sets out joint liability between assignors and assignees for any data treatment occurring after the transfer. The bill thus proposes the implementation of a regime similar to the one currently in place in South Africa.

Particularly important when it comes to the current regulatory regime on movement of data is a recently enacted sectoral law: the Brazilian Civil Rights Framework for the Internet (*Marco Civil da Internet*) and its regulating Decree No. 8771/2016. The *Marco Civil* contains a section regulating aspects of the protection of personal data processed online by connection providers and by Internet application providers.

Although the initial draft of the *Marco Civil* included provisions to nationalise data centres and restrict the cross-border movement of data (mainly in response to the Snowden revelations),[22] the final version of the law does not contain any provisions restricting international data transfers. Yet, according to the law, data subjects must

21 Thomson Reuters Practical Law, 'Data protection in Brazil: overview', 2017, https://uk.practicallaw.thomsonreuters.com/4-520-1732, accessed 8 March 2018.

22 Chander A & UP Lê, 'Breaking the Web: Data Localization vs. the Global Internet', UC Davis Legal Studies Research Paper, 378, April 2014.

provide their express consent regarding the collection, use, storage and processing of personal data (Article 7, Section IX). Consent cannot be implied and must be made in a specific clause separate from the remainder of the agreement or the terms of use. There is thus a requirement of consent at the moment of collection and processing, but there is no discrimination as to whether the data is processed inside or outside Brazil.

In summary, the protection of personal data is currently regulated under the *Marco Civil*, which is still limited when compared to the complex system envisaged by the data protection bill. While the *Marco Civil* does not impose any restrictions on cross-border data transfers, the new bill is likely to impose a conditional flow regime in the country.

In addition, there are two new proposed regulations that aim at restricting the location of storage and processing of data when using cloud computing solutions. The two proposals cover public procurement of cloud computing and usage of cloud computing by financial institutions and other institutes regulated by the Brazilian Central Bank.[23]

China[24]

The Internet – and cross-border data flows – is seen in China as an important strategic issue in terms of geopolitics and public order. China imposes overlapping horizontal and sector-specific restrictions related to electronic data processing, on both personal and non-personal information. Generally, it imposes a requirement to localise data, where companies must store any data they collect in China on servers located in the country. This requirement has been implemented since the early 1990s, despite not being formalised in written law and recognised as a *de facto* obligation.[25]

The recent Cybersecurity Law, derived from the Secure and Controllable Policy, formalises this overarching data localisation requirement.[26] This new law, which

23 BSA, 'Country: Brazil', http://cloudscorecard.bsa.org/2018/pdf/country_reports/2018_Country_Report_Brazil.pdf, accessed 8 March 2018; *The Washington Post*, 'The US dominates the world of big data. But Trump's NAFTA demands could put that at risk', 27 November 2017, https://www.washingtonpost.com/business/economy/trumps-trade-deficit-obsession-could-hurt-leading-american-industries/2017/11/27/b2b8122c-cbb5-11e7-8321-481fd63f174d_story.html?utm_term=.eeb250c431fe, accessed 8 March 2018.

24 The main source for this section is Ferracane MF & H Lee-Makiyama, 'China's Technology Protectionism and Its Non-negotiable Rationales', ECIPE Trade Working Paper, 2/2017, 2017, http://ecipe.org//app/uploads/2017/06/China-Tech-Protectionism.pdf, accessed 7 August 2017.

25 Business Roundtable, 'Promoting Economic Growth through Smart Global Information Technology Policy: The Growing Threat of Local Data Server Requirements', July 2012.

26 Standing Committee of the National People's Congress, Cybersecurity Law, 7 November 2016.

entered into force in June 2017, 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 KIIOs need to transfer this data outside of China for business reasons, security assessments must be conducted. The definition of KIIOs is not finalised yet, giving another example of ambiguity that could provide policy space for discrimination.[27]

In addition to horizontal regulations, there are also a number of sectoral regulations. Sensitive data such as personal information collected by commercial banks and population health information must be stored, handled and analysed within the territory of China, and is not allowed to be transferred and stored overseas.[28] In addition, online mapping service providers must set up their server inside the country, and must acquire an official certificate.[29] In 2016 China also instituted a licensing system for online taxi companies, which requires them to host user data on Chinese servers.[30]

In addition to specific requirements for processing data within the country, China also imposes conditions on the transfer of all personal data abroad, requiring the express consent of the data subject, government permission or explicit regulatory approval.[31]

Other Chinese regulations facilitate the government's access to data processed within the country. The State Security Law requires that the state security organ should always be permitted to access, when necessary, any information held by companies in China.[32] Unlike other jurisdictions, no due process of warrants or other jurisdictional checks are needed in order to access electronic communications.

27 Piper DLA, 'Data Protection Laws of the World: China', https://www.dlapiperdataprotection.com/index.html?t=law&c=CN, accessed 3 August 2017.

28 People's Bank of China, 'Notice to Urge Banking Financial Institutions to Protect Personal Financial Information', 21 January 2011.

29 China, State Council, *Map Management Regulations*, 14 December 2015.

30 China, Ministry of Transport, Ministry of Industry and Information Technology, Ministry of Public Security, Ministry of Commerce, State Administration for Industry and Commerce & General Administration of Quality Supervision, *Interim Measures for the Administration of Online Taxi Booking Business Operations and Services*, 28 July 2016.

31 General Administration of Quality Supervision, Inspection and Quarantine of China & Standardization Administration of China, *Guidelines for Personal Information Protection Within Public and Commercial Services Information Systems*, Article 5.4.5, 5 November 2012.

32 Article 11 of the State Security Law stipulates that 'where state security requires, a state security organ may inspect the electronic communication instruments and appliances and other similar equipment and installations belonging to any organization or individual'. Article 18 states that '[w]hen a State security organ investigates and finds out any circumstances endangering State security and gathers related evidence, citizens and organizations concerned shall faithfully furnish it with relevant information and may not refuse to do so'. See also Wang Z, 'Systematic government access to private-sector data in China', *International Data Privacy Law*, 2, 4, 2012.

In addition, the recently adopted Counter-Terrorism Law requires Internet service providers (ISPs) and the telecommunications sector to 'provide technical support and assistance, such as technical interface and decryption, to support the activities of the public security and state security authorities in preventing and investigating terrorist activities'.[33] At the same time, ISPs are already keeping records of each service user's time spent online, user account, IP address or domain name, phone number and other information for 60 days, and provide that information to government authorities when required.[34]

India

There is no specific legislation on privacy and data protection in India. However, the Information Technology Act of 2000 contains certain provisions intended to protect electronic data – including non-electronic records or information that has been, is currently or is intended to be processed electronically.[35] In April 2011 India's Information Technology Ministry adopted the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules implementing certain provisions of the Information Technology Act.[36]

The rules require corporate entities collecting, processing and storing personal data, including sensitive personal information, to comply with certain procedures. Cross-border flows of sensitive personal data or information[37] can be made only in three cases:

- if the receiving party ensures the same level of protection as that provided under Indian rules;
- 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.

33 China, Standing Committee of the National People's Congress, *Counterterrorism Law of the People's Republic of China*, Order of the President of the People's Republic of China, 36, 27 December 2015.

34 China, State Council, *Regulation on Internet Information Service of the People's Republic of China*, Decree of the State Council of the People's Republic of China 292, Article 14.

35 India, Information Technology Act of 2000 (Act 21 of 2000).

36 India, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

37 The Privacy Rules define 'sensitive personal data or information' to include information relating to passwords; financial information such as bank account, credit/debit card or other payment instrument details; physical, physiological and mental health conditions; sexual orientation; medical records and history; biometric information; any detail relating to the above clauses as provided to a corporate entity for providing services; and any of the information received under the above clauses for storing or processing under lawful contract or otherwise.

Specifically, Rule 7 provides:

> A body corporate or any person [acting] on its behalf may transfer sensitive personal data or information including any information, to any other body corporate or a person in India, or located in any other country, that ensures the same level of data protection that is adhered to by the body corporate as provided for under these Rules. The transfer may be allowed only if it is necessary for the performance of the lawful contract between the body corporate or any person on its behalf and provider of information or where such person has consented to data transfer.[38]

At the same time, there are precedents of forced localisation of data servers within Indian territory (eg, BlackBerry mail services in 2012), and today certain restrictions apply in the public sector. In 2012 India enacted the National Data Sharing and Accessibility Policy,[39] 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.[40]

Moreover, Section 4 of the Public Records Act of 1993 prohibited public records from being transferred out of Indian territory, except for 'public purposes':[41]

> 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.

Under the statute, 'any ... material produced by a computer' constitutes public records. In 2013 the Delhi High Court interpreted this requirement to bar the transfer of government emails outside India.[42] This was followed by a new email policy that regulates the use of government email services for government officials.[43] The policy states: 'Forwarding of e-mail from the e-mail id provided by GoI [Government of

38 India, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

39 India, Department of Science and Technology, National Data Sharing and Accessibility Policy (NSDAP), 2012.

40 Cory N, 'Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?', ITIF (Innovation Technology Innovation Foundation), 1 May 2017, https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost, accessed 13 August 2017.

41 India, Public Records Act 69 of 1993, Indian Code (1993).

42 *KN Govindacharya v. Union of India and ORS*, W.P.(C) 3672/2012, CM Nos. 7709/2012, 12197/2012 and 6888/2013, High Court of Delhi (20 October 2013), http://delhihighcourt.nic.in/dhcqrydisp_O.asp?pn=163416&yr=2013, accessed 13 August 2017.

43 India, Ministry of Communication & Information Technology, *E-mail Policy of Government of India*, October 2014, Version 1.0. F. No. 2(22)/2013-EG-II, http://meity.gov.in/writereaddata/files/E-mail_policy_of_Government_of_India_3.pdf, accessed 13 August 2013.

India] to the Government official's personal id outside the GoI email service is not allowed due to security reasons.'[44]

In January 2014 the media reported on a leaked internal note from the National Security Council Secretariat, which showed that the government was considering a three-pronged strategy with strong elements of data localisation.[45] The proposal included mandating all email providers to set up local servers for their India operations such that 'all data generated from within India should be hosted in these India-based servers and this would make them subject to Indian laws'.[46] There was no follow-up to the proposal.

Finally, in 2015 India released a National Telecom Machine-to-Machine Roadmap that requires all relevant gateways and application servers that serve customers in India to be located in India. The roadmap has not been implemented yet.[47] However, in the same year India's Ministry of Electronics and Information Technology issued guidelines for a cloud computing empanelment process under which cloud computing service providers may be provisionally accredited as eligible for government procurement of cloud services. The guidelines require such providers to store all data in India to qualify for the accreditation.[48]

Overall, the current regime is similar to that of South Africa and the one proposed in Brazil, in which data can flow freely cross-border if certain conditions are fulfilled. However, the country has strict localisation rules for certain government services, and is considering additional rules.

Russian Federation

The Russian Federation, like China, is among the most restrictive countries in the world when it comes to moving data cross-border. Data protection in Russia has been covered since 27 July 2006 by Federal Law No. 152-FZ, also known as the OPD Law ('On Personal Data').[49] In July 2014 the law was amended by Federal Law

44 *Ibid.*

45 Thomas TK, 'National Security Council proposes 3-pronged plan to protect Internet users', *The Hindu Business Line*, 13 February 2014, http://www.thehindubusinessline.com/info-tech/national-security-council-proposes-3pronged-plan-to-protect-internet-users/article5685794.ece, accessed 13 August 2013.

46 *Ibid.*

47 Cory N, *op. cit.*

48 India, Ministry of Electronics and Information Technology, 'Guidelines for Government Departments On Contractual Terms Related to Cloud Services', 31 March 2017, http://meity.gov.in/writereaddata/files/Guidelines-Contractual_Terms.pdf, accessed 10 March 2018.

49 Russia, State Duma, Russian Federal Law on Personal Data (No. 152-FZ), 8 July 2006.

No. 242-FZ to include a clear data localisation requirement.[50] 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 are made using databases located in the country. This amendment entered into force on 1 September 2015.

Online websites that violate the prohibition could be placed on a blacklist by the Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor). It is not clear how restrictive the data localisation requirement is, but it seems that the OPD Law does not prohibit accessing servers from abroad or impose any special restrictions on cross-border data transfers or duplication of personal data. In any case, the law is considered among the most comprehensive and restrictive in the world, and – if implemented to the letter – would have significant impact on the provision of online services to the country.

In addition to the OPD Law, Russia has additional local storage and processing requirements that target specific data or businesses. First, amendments to the National Payment System Law in October 2014 require international payment cards to be processed locally.[51] International payment systems had to transfer their processing capabilities with respect to Russian domestic operations to the local state-owned operator (National Payment Card System) by March 2015.[52] The amendments are reported to be a response to the international political sanctions that prohibited certain international payment systems (eg, Visa and MasterCard) from servicing payments on cards issued by sanctioned Russian banks.

Federal Law No. 374-FZ, signed in July 2016, requires local storage (but not processing) for a period of three years (with respect to telecom providers) or one year (with respect to Internet arrangers) of information confirming the *fact* of receipt, transmission, delivery and/or processing of voice data, text messages, pictures, sounds, video or other communications (ie, metadata reflecting these communications).[53] In addition, local storage for a period of six months is required

50 Russia, Federal Law 21.07.2014 No. 242-FZ On the Amendment of Certain Legislative Acts of Russian Federation Concerning the Procession of Personal Data in Computer Networks, July 2014.

51 Russia, Federal Law No. 319-FZ On Amendments to the Federal Law on the National Payment System and Certain Legislative Acts of the Russian Federation, 22 October 2014.

52 Dentons, 'International payment cards processing: From Russia with love', 11 November 2014, http://www.dentons.com/en/insights/alerts/2014/november/11/international-payment-cards-processing-from-russia-with-love, accessed 7 August 2017.

53 Russia, Federal Law No. 374-FZ On the Introduction of Amendments to Federal Law 'On the Counteraction of Terrorism' and to Certain Legislative Acts of the Russian Federation with Regard to Establishing Additional Measures Designed to Counteract Terrorism and Promote Public Safety, 6 July 2016; Koroleva K, '"Yarovaya" Law – New Data Retention Obligations for Telecom Providers and Arrangers in Russia', Global Privacy & Security Compliance, Law Blog, 29 July 2016, https://www.globalprivacyblog.com/privacy/yarovaya-law-new-data-retention-obligations-for-telecom-providers-and-arrangers-in-russia/, accessed 10 March 2018.

for the *contents* 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 comes into force in July 2018.

Earlier in August 2014, the Russian government had issued a decree requiring public Wi-Fi user identification.[54] The decree states that:

- ISPs should identify Internet users, by means of identity documents (such as passports);
- ISPs should identify terminal equipment by determining the unique hardware identifier of the data network; and
- all legal entities in Russia should provide ISPs each month with a list of the individuals who connected to the Internet using their network.

This data should be stored locally for a period of at least six months. Later in 2015 the authorities proposed fines for non-compliance of up to RUB 200,000 (approximately $2,600) for legal entities. The fines would be higher for repeating offenders.

Finally, a conditional flow regime has been in place under the OPD Law since 2007. According to the law, the transfer of data outside Russia does not require additional consent from the data subject *only* if the jurisdiction to which the personal data is transferred ensures adequate protection. Those jurisdictions are the parties to the Convention 108 and other countries approved by Roskomnadzor. The official list of countries includes Australia, Argentina, Canada, Israel, Mexico and New Zealand.

THE COSTS OF DATA LOCALISATION

Several studies point out the costs to local businesses and the local economy of restricting data flows. In fact, businesses rely heavily on cross-border data flows for a number of purposes, from managing a global workforce to monitoring production systems. Companies also collect and analyse customers' data from all over the world to better understand preferences and adapt products and services accordingly.

Information, especially as a result of developments in cloud computing and big data, is today routed automatically and autonomously across local routers that belong to the Internet network. The paths followed by data are determined purely by efficiency, and users often do not know where their data is physically stored and processed.

When data localisation measures apply, companies have to pay for more expensive or even duplicate services when they transfer data needed for day-to-day activities, for example for human resources management. Moreover, local companies incur

54 Reuters, 'Russia demands Internet users show ID to access public Wifi', 8 August 2014, http://www.reuters.com/article/us-russia-internet-idUSKBN0G81RV20140808, accessed 7 August 2017.

higher costs when accessing foreign data processing services. Measures imposing restrictions on data therefore impact the productivity of firms not only in the digital sector but also in virtually any sector of the economy. These costs are ultimately borne by customers or local firms. As mentioned in a report by the Swedish National Board of Trade, 'trade cannot happen without data being transferred from one location to another'.[55]

Measures imposing restrictions on data therefore impact the productivity of firms not only in the digital sector but also in virtually any sector of the economy

This section presents a summary of the most relevant studies on data flow restrictions and their impact on the economies that have implemented them. Each sub-section addresses a specific variable, namely jobs; cost of data processing; access to innovation; macroeconomic impact on productivity, investment and growth; cost for third countries; and the non-economic implications of data localisation regimes.

Jobs

Some countries have imposed data localisation requirements in the belief that such rules would force companies to relocate data-related jobs to their territories. However, this has proven not to be the case. Jobs associated with data centres have been decreasing sharply as data centres become more automated. Data centres contain expensive hardware that is often imported[56] and create construction work only in the short term while employing relatively few full-time staff.

This is confirmed by several studies. A 2008 report found that Yahoo, Ask.com, Intuit and Microsoft had hired a total of 180 workers for their facilities – an average of 45 workers per facility.[57] Other media reports from 2011 showed that a massive $1 billion data centre Apple built to help power its cloud computing products

55 Swedish National Board of Trade, 'No Transfer, No Trade: The Importance of Cross-Border Data Transfer for Companies based in Sweden'. Stockholm: Kommerskollegium, 2014.

56 Cory N, *op. cit.*

57 Miller R, 'The economics of data center staffing', Data Center Knowledge, 18 January 2008, http://www.datacenterknowledge.com/archives/2008/01/18/the-economics-of-data-center-staffing/, accessed 6 August 2017; Ohara D, '# of data center employees (Yahoo, Ask.com, Intuit, and Microsoft) in Washington Columbia Basin', Green Data Center & Wireless Blog, 10 January 2008, http://www.greenm3.com/gdcblog/2008/1/11/of-data-center-employees-yahoo-askcom-intuit-and-microsoft-i.html, accessed 6 August 2017.

created only 50 new full-time jobs.[58] In 2015 the media reported that Apple's $2 billion global command centre in Mesa, Arizona would employ 150 full-time personnel, and create between 300 and 500 construction and trade jobs.[59]

The number of jobs created is thus quite limited and, as shown in the following sections, these benefits are more than outweighed by losses in productivity and growth in the local economy.

Costs of data processing

Restrictions on movement of data cross-border are associated with increased data processing costs, which local companies have to bear. Companies are likely to spend more on data storage services if data has to be processed within the country. A study by the Leviathan Security Group finds that in many countries that are considering

Restrictions on movement of data cross-border are associated with increased data processing costs, which local companies have to bear

or have considered forced data localisation laws, local companies would be required to pay 30–60% more for their computing needs than if they used services located outside the country's borders.[60] Resources are therefore diverted from other investments that the company could make – including hiring new employees and buying new equipment.

The methodology used by the Leviathan Security Group compares the prices offered by local providers with the cheapest secure alternative option offered worldwide. In Brazil, for example, at the low end for 1GB-equivalent servers, Microsoft's price in 2015 was $0.024/hour. The lowest worldwide price for 1GB-equivalent servers – $0.015/hour – would save Brazilian customers 37.5% on their server costs when compared to a Brazil-exclusive solution. For a 2GB-equivalent server,

58 Blodget H, 'The country's problem in a nutshell: Apple's huge new data center in North Carolina created only 50 jobs', *Business Insider*, 28 November 2011, http://www.businessinsider.com/apple-new-data-center-north-carolina-created-50-jobs-2011-11, accessed 10 March 2018; Rosenwald MS, 'Cloud centers bring high-tech flash but not many jobs to beaten-down towns', *The Washington Post*, 24 November 2011, http://www.washingtonpost.com/business/economy/cloud-centersbring-high-tech-flash-but-not-manyjobs-to-beaten-down-towns/2011/11/08/gIQAccTQtN_story.html, accessed 10 March 2018.

59 Etherington D, 'Apple to build a $2 billion data command center in Arizona', *TechCrunch*, 2 February 2015, https://techcrunch.com/2015/02/02/apple-to-build-a-2-billion-data-command-center-in-arizona/, accessed 10 August 2017.

60 Leviathan Security Group, 'Quantifying the Cost of Forced Localization', 2015, https://static1.squarespace.com/static/556340ece4b0869396f21099/t/559dad76e4b0899d97726a8b/1436396918881/Quantifying+the+Cost+of+Forced+Localization.pdf, accessed 10 August 2017.

a Brazil-located solution would cost $0.08/hour, and the cheapest price globally would be $0.03/hour – a saving of 62.5%. Averaged across the types of servers, a customer located in Brazil would pay 54.6% less by using cloud servers outside Brazil instead of Brazil-located cloud computing resources.

Another example is the EU. Some people in the EU have called for a 'European cloud', limiting data processing to data centres in the Schengen area.[61] The Leviathan study finds that, if a European cloud were put in place, cloud computing at 4GB and above would be consistently 10.5% more expensive than accessing cheaper alternatives worldwide. However, for 1GB and 2GB services companies would not have to pay more, as the world's lowest-cost data centres were located in the EU in 2015, when the study was done.

Access to innovation

Barriers to data flows create delays and higher costs for accessing innovative goods and services that rely on cross-border flow of data. Therefore, these measures make it more expensive for local companies to gain exposure and benefit from the ideas, research, technologies and best practices that accompany data flows.[62] In addition, creating new businesses that rely on other global services becomes more expensive or even impossible. The resultant delays and costs are borne by local businesses and consumers.[63] This is especially the case when it comes to new innovative solutions that rely on the distributed nature of the Internet and the aggregation of data, such as big data analytics, cloud computing and the Internet of Things.

Macroeconomic impact on productivity, investment and growth

As mentioned above, data localisation benefits a small number of local companies offering data processing services, while creating significant costs for the entire economy. The domestic benefits of data localisation accrue to a few data centre owners and employees, while the costs are widespread and affect all businesses and consumers that are denied access to certain global services. The additional costs of processing data and accessing innovation have a trickle-down impact on the macroeconomic performance of those countries implementing such rules. Eventually, these measures are likely to have a negative impact on businesses and consumers with fewer resources, thereby increasing poverty and inequality.

61 The Schengen area includes all EU member states, with the exception of the UK and Ireland, and includes some non-EU countries, ie, Norway, Iceland, Switzerland and Liechtenstein.

62 Cory N, *op. cit.*

63 See, among others, successful Indian companies such as Slideshare and Zoho, which rely on services such as Amazon Web Services or Google Apps.

The first comprehensive study that attempted to quantify the macroeconomic impact of data localisation was conducted by ECIPE in 2014.[64] The authors developed an empirical model to estimate the impact of proposed or enacted data localisation rules and related laws on data privacy in Brazil, China, the EU, India, Indonesia, the Republic of Korea and Vietnam.[65]

ECIPE's study measures the impact of data rules on exports, gross domestic product (GDP) and lost consumption owing to higher prices and displaced domestic demand. The impact of proposed or enacted data restrictions on GDP is found to be substantial in all seven countries analysed in the study: Brazil (-0.2%), China (-1.1%), EU (-0.4%), India (-0.1%), Indonesia (-0.5%), the Republic of Korea (-0.4%) and Vietnam (-1.7%).[66] If these countries also introduced economy-wide data localisation requirements, GDP losses would be even higher: Brazil (-0.8%), the EU (-1.1%), India (-0.8%), Indonesia (-0.7%) and the Republic of Korea (-1.1%).

The impact on domestic investments is also considerable: Brazil (-4.2%), China (-1.8%), the EU (-3.9%), India (-1.4%), Indonesia (-2.3%), the Republic of Korea (-0.5%) and Vietnam (-3.1%). If these countries also introduced economy-wide data localisation, the impact increased for most: Brazil (-5.4%), the EU (-5.1%), India (-1.9%), Indonesia (-12.6%), the Republic of Korea (-3.6%) and Vietnam (-3.1%). Exports from China and Indonesia decreased by 1.7% owing to loss of competitiveness.

If these countries enacted economy-wide data localisation, the study estimates that higher prices and displaced domestic demand would lead to consumer welfare losses of $15 billion for Brazil, $63 billion for China, $193 billion for the EU, $14.5 billion for India, $3.7 billion for Indonesia, $15.9 billion for the Republic of Korea and $1.5 billion for Vietnam. For India, the loss per worker is equivalent to 11% of the average monthly salary; in China this is almost 13%, and around 20% in the Republic of Korea and Brazil.

64 Bauer M *et al.*, 'The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce', ECIPE, March 2013, https://www.uschamber.com/sites/default/files/documents/files/020508_EconomicImportance_Final_Revised_lr.pdf, accessed 13 August 2017; Bauer M *et al.*, 'The Costs of Data Localisation: Friendly Fire on Economic Recovery', ECIPE Occasional Paper, 3/2014, March 2014, http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf, accessed 13 August 2017. In 2013 ECIPE also conducted a preliminary analysis on the impact of the proposed GDPR on the EU economy and on EU–US services trade. See Bauer M *et al.*, *op. cit.*

65 Beyond data localisation, the study also considers other common regulatory requirements for data protection that increase compliance costs, such as strict consent requirements for data use and transfers, a right for users to review personal data, strict requirements to notify authorities of data breaches, the appointment of a data privacy officer, sanctions for noncompliance, and the requirement to provide government access to a business's or its customers' data.

66 This represents a one-time shock on the GDP of the country; that is, GDP is systematically lower than it could have been if there were no restrictions in place.

Another study published in 2016 shows that strict rules on data (including data localisation) increase prices and lower productivity in a range of economies.[67] The regulatory measures addressed in the analysis cover both restrictions on foreign supply of data services and restrictions connected to internal productivity losses and administrative costs (Table 1).

TABLE 1 TYPES OF REGULATORY MEASURES RESTRICTING DATA SERVICES

TYPE OF RESTRICTION	REGULATORY MEASURE	OUTCOME
Restrictions related to the foreign supply of data services	Is there a data localization requirement?	Yes/Limited/No
Restrictions related to internal productivity losses/ administrative costs	Is there a strict consent requirement for the collection, storage or dissemination of personal data?	Yes/No
	Does the law provide users with the right to review their stored information?	Yes/No
	Does the law provide users with the right to be forgotten/deleted?	Yes/No
	Is there a notification of breaches toward the government/user obligatory?	Toward government/ user/government and user
	Are data protection impact assessments obligatory?	Yes/No
	Is a data protection officer required?	Yes/No/Qualified yes
	Are there administrative sanctions for non-compliance? How high?	Varies according to height of sanctions
	Does the government require easy access to companies' data?	Yes/No
	Are companies required to retain data for a fixed period of time?	Yes/No

Source: Bauer M, Ferracane MF & E Van der Marel, 'Tracing the Economic Impact of Regulations on the Free Flow of Data and Data Localisation', CIGI and Chatham House, Global Commission on Internet Governance Paper 30, May 2016, https://www.cigionline.org/publications/tracing-economic-impact-regulations-free-flow-data-and-data-localization, accessed 13 August 2017

The authors investigated which of the regulatory measures identified were implemented in eight economies (Brazil, China, the EU, India, Indonesia, the Republic of Korea, Russia and Vietnam), and created a cost index that summarises

67 Bauer M, Ferracane MF & E Van der Marel, 'Tracing the Economic Impact of Regulations on the Free Flow of Data and Data Localisation', CIGI (Centre for International Governance Innovation) & Chatham House, Global Commission on Internet Governance Paper, 30, May 2016a, https://www.cigionline.org/publications/tracing-economic-impact-regulations-free-flow-data-and-data-localization, accessed 13 August 2017.

the economy's regulatory environment on data flows. Another important piece of the analysis is the measurement of the data intensity of downstream sectors in the economy. These two measures – data regulations index and data intensity – form a joint indicator for an econometric analysis that estimates the economic impact of the measures via change in total factor productivity (TFP).

The results show that the negative impact of data-related measures on the economies analysed is substantial. The lost TFP in downstream sectors, especially services, reduces GDP by up to 0.58% in the case of the Republic of Korea (see Table 2).

The most recent study on the macroeconomic impact of data localisation and data-related rules was released by ECIPE in late 2016.[68] The study shows that data localisation diminishes productivity, and that this impact far outweighs any marginal gains for the domestic ICT sector from restrictions on movement of data. The econometric study focuses on EU data localisation measures to estimate the economic benefits for EU countries if the restrictions were lifted, as well as the additional costs if the measures grew into full data-localisation measures between EU members.

TABLE 2 SIMULATION RESULTS AND PERCENTAGE CHANGES IN REAL GDP

EU	-0.48
Brazil	-0.10
China	-0.55
India	-0.25
Indonesia	-0.23
Korea	-0.58
Vietnam	-0.24

Source: Bauer M, Ferracane MF & E Van der Marel, 'Tracing the Economic Impact of Regulations on the Free Flow of Data and Data Localisation', CIGI and Chatham House, Global Commission on Internet Governance Paper 30, May 2016, https://www.cigionline.org/publications/tracing-economic-impact-regulations-free-flow-data-and-data-localization, accessed 13 August 2017

The study finds 22 cases in which EU member countries impose direct restrictions on the transfer of data to other EU members. These measures are used to estimate 'best-case' and 'worst-case' scenarios for the economy. In the best-case, 'liberalisation' situation, actual data localising measures in the EU are removed (considering the price and productivity impact), and a worst-case 'ratchet' situation looks at the economy-wide cost in terms of lost productivity if all cross-border data flows within the EU were restricted.

68 Bauer M *et al.*, 'Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States', ECIPE Policy Brief, 3/16, March 2016b, http://ecipe.org//app/uploads/2016/12/Unleashing-Internal-Data-Flows-in-the-EU.pdf, accessed 13 August 2017.

The best-case scenario estimates that the removal of existing data-localisation policies would increase GDP by 0.05% in the UK and Sweden, 0.06% in Finland, 0.07% in Germany, 0.18% in Belgium and 1.1% in Luxembourg. In a situation with clear and unfettered competition in the EU for data services, the authors estimate the EU's GDP to increase by up to 0.06%. These results likely underestimate the impact of data localisation, as implicit or indirect data localisation measures are not included.

The worst-case scenario estimates that full data localisation policies would remove 0.4% from the EU economy each year. The impact varies in individual countries, ranging from -0.27% of GDP in Croatia to -0.61% of GDP in Luxembourg. The impact depends on the size of each country's data-intensive and services sectors. Given this, it is unsurprising that the impact is particularly pronounced on the ICT sector. The study estimates that the loss in output in the ICT sector ranges from 0.54% in Poland to 3.46% in Luxembourg.

Cost for third countries

Data localisation rules not only represent a 'self-inflicted' sanction on the economies that implement them but also have clear costs for foreign companies and, in turn, foreign economies. This is because the costs of exporting to the country that is implementing data localisation rules increase significantly, and as a result certain companies might even decide to leave the country.

This was confirmed by a 2014 study by the US International Trade Commission.[69] The study shows that barriers to digital trade and data flows imposed significant costs on US firms and the US economy. The study estimated an increase in GDP of up to $41.4 billion were foreign barriers on digital trade removed.[70]

The imposition of data localisation measures can also give rise to retaliatory behaviour from trading partners, harming consumers and businesses alike in all countries involved.

69 USITC (US International Trade Commission), 'Digital Trade in the US and Global Economies, Part 2', August 2014, https://www.usitc.gov/publications/332/pub4485.pdf, accessed 27 August 2017.

70 The econometric model used surveys of US firms in these sectors to identify barriers to digital trade and to rank countries that enact these barriers in order to help the model estimate the impact removing these barriers would have on these sectors and the overall US economy. The USITC sent questionnaires to a stratified random sample of nearly 10 000 firms in seven digitally intensive industries. The questionnaires asked firms how they used the Internet and how the Internet had changed their business practices, sales and productivity. The questionnaires also asked firms about their experiences with foreign barriers and impediments to digital trade. The survey had a response rate of nearly 41%. Of the more than 3 600 companies that responded, 80% were small and medium enterprises (SMEs).

Non-economic implications connected to restrictions on data flows

From the analysis above, it is clear that there is little economic rationale for data localisation, and the current wave of digital protectionism cannot be justified on those grounds. Domestic rationales often appear to be non-economic, such as avoiding foreign surveillance, promoting law enforcement, protecting data privacy or enhancing cybersecurity.

While there is some truth to this argument, it is often possible to find less trade-restrictive alternatives that can achieve such domestic policy objectives through alternative solutions that let data flow freely across borders. In addition, restrictions to movement of data cross-border can have detrimental effects on data security. While an in-depth discussion of these arguments is beyond the scope of this paper, this section does offer a brief justification.

Data localisation measures fail to take into account the advances brought about by the distributed nature of the Internet, distributed packets and encryption of data for security reasons.[71] Data security is not a function of data's physical storage but rather of the technical, administrative and physical controls implemented by the service provider, including the strength of the encryption techniques used – regardless of where the data centre is located.[72]

Compelling companies to use local data centres increases the likelihood of choosing companies with weak security measures, as the company has a smaller range of choices. Usually, strong security controls on cloud computing are best offered by large-scale providers. Allowing firms to access those providers can best guarantee the security of data, rather than requiring small and medium-sized businesses to develop their own security solutions.

Security risks would also be exacerbated by the scarcity of cybersecurity talent in certain countries that want to impose data localisation. In addition, when countries that impose data localisation are at risk of natural disasters, the risks are further increased by the impossibility of replicating the data lost in such an event. This is a basic principle of the Internet: route around damage in order to ensure that communication is never stopped. To protect users' data from large-scale natural disasters, it is often helpful to store data on multiple continents at the same time, so that an infrastructure breakdown in one place will not affect data integrity or availability elsewhere.[73]

71 European Commission, 'Staff Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy', 10 January 2017, https://ec.europa.eu/digital-single-market/en/news/staff-working-document-free-flow-data-and-emerging-issues-european-data-economy, accessed 23 August 2017.

72 Chander A & UP Lê, 2014, *op. cit.*; Chander A & UP Lê, 'Data nationalism', *Emory Law Journal*, 64, 3, 2015, pp. 677–739, http://law.emory.edu/elj/_documents/volumes/64/3/articles/chander-le.pdf, accessed 23 August 2017.

73 Leviathan Security Group, *op. cit.*

Weaker security makes systems easier to target – not only by cyber attacks but also by foreign surveillance. In fact, foreign surveillance by foreign governments cannot easily be avoided through data localisation. When it comes to the US, for example, surveillance efforts are often concentrated abroad.[74] Moreover, the use of malware eliminates the need to have operations on the ground in the countries where the surveillance occurs. In any case, governments themselves routinely share information with each other, even outside the official treaty procedures on sharing.[75]

Another concern is that data localisation rules can be abused by the implementing country to bypass domestic legal processes to access data. In fact, when locally stored, data might be more easily accessed by a government, which could therefore have greater control over both local information and its citizens.[76] The availability of data for lawful regulatory and supervisory purposes would be better ensured by enhancing cooperation between national authorities or between such authorities and the private sector.[77]

To conclude, another of the non-economic implications of strict restrictions is that they hamper citizens' ability to access information and reach international markets. This is owing to the delays and additional costs that citizens would encounter in accessing foreign services.

REGULATION OF DATA FLOWS IN FTAs AND AT THE MULTILATERAL LEVEL: THE CURRENT POLICY DISCUSSION[78]

Data policies are increasingly used as a protectionist measure, which means that cross-border data flows are also gaining more attention as a focus of trade policy. Until now, only a few free trade agreements (FTAs) have addressed such issues. The most relevant are the US–Korea FTA (KORUS), the EU–Korea FTA, and the more recent EU–Vietnam FTA and EU–Canada Comprehensive Economic and Trade Agreement (CETA). Moreover, the now-dead Trans-Pacific Partnership (TPP12) was the first agreement to include a general obligation to allow cross-border transfer of data and a ban on data localisation.

74 Chander A & UP Lê, 2015, *op. cit.*

75 *Ibid.*

76 Hon WK *et al.*, 'Policy, Legal and Regulatory Implications of a Europe-Only Cloud', Queen Mary University of London, School of Law, Legal Studies Research Paper, 191/2015, 2015, http://www.picse.eu/sites/default/files/PolicyLegalandRegulatoryImplicationsof%20EuropeOnlyCloud.pdf, accessed 11 August 2017.

77 European Commission, 2017, *op. cit.*

78 Ferracane MF, 'After TPP: The Making Up of Trade Rules for Data Flows', Borderlex PRO, Monthly Trade Briefing, April 2016, http://borderlex.eu/wp-content/uploads/2016/07/2016-04-BORDERLEX-PRO-MONTHLY.pdf, accessed 11 August 2017.

This section looks at the wording of these agreements, as well as of other agreements under negotiations such as the Transatlantic Trade and Investment Partnership (TTIP) and the Trade in Services Agreement (TiSA). Important initiatives such as the Cross-Border Privacy Rules (CBPRs) system proposed by the Asia-Pacific Economic Cooperation (APEC) and the EU Free Flow of Data Initiative (FDDI) are also mentioned, before concluding with some remarks on the jurisprudence of the World Trade Organization (WTO).

FTAs/AGREEMENTS IN FORCE

KORUS

The 2011 KORUS agreement is the first international treaty with binding rules on cross-border data flows. Article 15.8 of the agreement states that 'the Parties shall endeavor to refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders'.[79] The wording of the article suggests that the commitment is only hortatory and therefore there is not a specific obligation to refrain from imposing barriers to cross-border flows of data. Moreover, the commitment is further softened by the mention of the General Agreement in Trade and Services (GATS) exceptions under Article XIV, which would allow parties to adopt Internet restrictions (Article 23.1.2 of the KORUS). The KORUS also sets specific commitments on cross-border data flows related to financial services. Under Annex 13-B, the parties agreed to 'allow a financial institution of the other Party to transfer information in electronic or other form, into and out of its territory, for data processing where such processing is required in the institution's ordinary course of business'.[80]

EU–Korea FTA

The wording found in the EU–Korea FTA, which entered into force in 2011, is comparable. Under the electronic commerce section, the parties recognise the 'importance of avoiding barriers' to the use and development of electronic commerce and agree that such development should be 'fully compatible with the international standards of data protection' (Article 7.48),[81] while also providing the same GATS exceptions mentioned in KORUS (Article 7.50). Moreover, the parties undertook to allow financial institutions to transfer data abroad for processing (Article 7.43).

79 Free Trade Agreement between the European Union and its Member States, of the one Part, and the Republic of Korea, of the Other Part, 6 October 2010, 127, O.J.L 6, 2011 (hereafter EU–Korea FTA).

80 Free Trade Agreement between the United States of America and the Republic of Korea, 30 June 2007, 46 I.L.M. 642, entered into force March 15, 2012 (hereafter KORUS).

81 EU–Korea FTA, *op. cit.*

EU–Vietnam FTA and CETA

In the recently agreed text of the EU–Vietnam FTA, Section VI on financial services, the parties agreed to permit a financial service supplier of the other party to transfer data abroad for processing. Similarly, CETA includes an article in which the parties commit themselves to 'permit a financial institution or a cross-border financial service supplier of the other Party to transfer information in electronic or other form, into and out of its territory, for data processing if processing is required in the ordinary course of business of the financial institution or the cross-border financial service supplier' (Article 13.15).[82]

APEC Cross-Border Privacy Rules[83]

The CBPRs are based on the APEC Privacy Framework and have been endorsed by APEC leaders since 2011, with the objective to facilitate movement of data among APEC economies. The system is voluntary and accountability-based, and has four main components:

- recognition criteria for organisations wishing to become an APEC CBPR system-certified accountability agent;
- intake questionnaire for organisations that wish to be certified as APEC CBPR system-compliant by a third-party CBPR system-certified accountability agent;
- assessment criteria for use by APEC CBPR system-certified accountability agents when reviewing an organisation's answers to the intake questionnaire; and
- a regulatory cooperative arrangement to ensure that each of the APEC CBPR system programme requirements can be enforced by participating APEC economies.

FTAs/AGREEMENTS UNDER NEGOTIATION[84]

TPP12

The electronic commerce chapter of the TPP12 agreement presents for the first time a general obligation in an FTA to allow cross-border transfer of data, and

82 Comprehensive Economic and Trade Agreement between Canada of the One Part and the European Union and its Member States, if the other Part, Sept 14, 2016, 2016/206 (NLE), (consolidated text) (hereafter CETA).

83 For detailed information, see CBRP (Cross Border Privacy Rules System), http://www.cbprs.org/, accessed 3 August 2017.

84 Given its possible revival as the TPP11, the TPP12 agreement is included in this section. The EU–Japan agreement under negotiation is also likely to cover the issue of data flows. However, the language on data flows is not clear yet and therefore is not included in this section. This section also includes a mention of the EU Free Flow of Data Initiative, which aims at eliminating restrictions on movement of data intra-EU. See Vincenti D, 'EU–Japan one step closer to signing trade deal', Euractiv, 4 July 2017, https://www.euractiv.com/section/economy-jobs/news/eu-japan-one-step-closer-to-signing-trade-deal/, accessed 3 August 2017.

addresses three important areas relevant to cross-border data flows: data privacy, access to software source code, and data localisation. The original agreement with 12 countries is now defunct because of the US' withdrawal. However, the language might be used again in various other agreements, including the TPP11. According to major industry representatives, TPP trade provisions can become the '*de facto* floor for digital trade rules' in other trade agreements such as TiSA and TTIP.[85]

Article 14.11 on Cross-Border Transfer of Information by Electronic Means is the core element in the new digital trade architecture forged by the TPP. The article states that 'each Party shall allow the cross-border transfer of information by electronic means, including personal information'.[86]

The agreement also presents the possibility of exceptions to this rule in order to achieve 'a legitimate public policy objective', provided that a measure:

(a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and

(b) does not impose restrictions on transfer of information greater than are required to achieve the objective.

Such exceptions follow those listed in Article XIV of the GATS, but remain rather general by not listing all the cases that would constitute a legitimate public policy objective.

In the data privacy area, the TPP calls for each party to 'adopt or maintain a legal framework that provides for the protection of the personal information of the users of electronic commerce',[87] as it recognises that such frameworks play a crucial role in protecting the integrity of cross-border data flows and people's trust in such flows (Article 14.8). Moreover, the agreement does not list specific privacy principles that should be adopted or a particular regulatory regime. It therefore gives the parties considerable flexibility to pursue privacy principles.[88] Also of relevance when it comes to data flows is Article 14.17 of the electronic commerce chapter, which prevents a country from making access to source code a condition of conducting

85 SIIA (Software and Information Industry Association), 'SIIA testifies before ITC: Says TPP will ensure digital trade works for US companies', 13 January 2016, http://www.siia.net/Press/SIIA-Testifies-Before-ITC-Says-TPP-will-Ensure-Digital-Trade-Works-for-US-Companies, accessed 30 August 2017.

86 Office of the US Trade Representative, 'TPP: Full text', 4 February 2016, https://ustr.gov/trade-agreements/free-trade-agreements/trans-pacific-partnership/tpp-full-text, accessed 20 December 2017.

87 *Ibid.*

88 In particular, Article 14.18 specifies that a party may comply with privacy protection obligations 'by adopting or maintaining measures such as a comprehensive privacy, personal information or personal data protection laws, sector-specific laws covering privacy, or laws that provide for the enforcement of voluntary undertakings by enterprises relating to privacy'.

business. However, this protection does not extend to software used for so-called 'critical infrastructure'.[89]

An extremely relevant and timely provision in the TPP text is the prohibition on forced localisation of server capacity, which directly relates to the general obligation to allow cross-border transfers of data presented above. Given that data localisation provisions have been mushrooming all over the world, governments are addressing them more explicitly in trade negotiations. Article 14.13 on the Location of Computing Facilities specifies that '[n]o Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory'.[90] Particularly interesting is the presence of the verbs 'using' and 'locating'. Data localisation measures, in fact, can take different forms, including the requirement to build data servers in the implementing country (as is the case in Vietnam, for example) or the requirement to use servers located within a certain jurisdiction (as in China or Russia).

In the TPP, exceptions to the prohibition are permitted in order to achieve a legitimate public policy objective, but they cannot be disguised restrictions on trade and must be the least restrictive measure possible. Yet the TPP does not explain what constitutes a legitimate public policy objective, leaving the door open to certain restrictions on cross-border data flows, notably under the national security exception. The TPP also excludes financial services from the ban on data localisation requirements.[91]

TTIP

The TTIP's forced hibernation owing to political changes in the US might soon come to an end.[92] Movement of data has been an especially sensitive issue between the US and the EU, and it is worth looking into the state-of-play before negotiations were halted. The US Trade Representative had already set out cross-border data flow objectives, seeking to 'include provisions that facilitate the movement of cross-border data flows' on the grounds that 'free flows of data are critical components of

89 'Critical infrastructure' is software deemed critical for public safety, but its definition is open to interpretation. Stewart Baker, former general counsel at the NSA, argues that the ban does not apply, for example, to code run on critical infrastructure. This could lead to disputes, as little mass market software does not run on computers involved in critical infrastructure.

90 Office of the US Trade Representative, *op. cit*.

91 This issue is regulated in a separate chapter dedicated to financial services (Chapter 11): financial data may flow internationally, and each country shall permit the transfer and processing of financial data by another country's financial service supplier. Yet the TPP's financial services carve-out enables countries to mandate that financial records are stored locally.

92 LaRocco LA, 'Wilbur Ross says he's "open to resuming" talks on mega-trade deal with Europe', CNBC, 30 May 2017, https://www.cnbc.com/2017/05/30/exclusive-wilbur-ross-says-hes-open-to-resuming-ttip-negotiations.html, accessed 14 August 2017.

the business model for service and manufacturing enterprises in the US and the EU and key to their competitiveness'.[93]

The US has proposed data flow rules in the e-commerce chapter of the TTIP that are similar to those proposed in TiSA. Yet, despite the fact that the mandate given to the European Commission by EU member states also covers data flows, negotiations on this topic have not started yet under the TTIP. Discussions were originally delayed because of the sensitive on-going discussions regarding the EU's new GDPR, which was adopted in April 2016 by the EU Parliament, and the Privacy Shield, which entered its implementation phase in the same period. The Privacy Shield came into force in July 2016, but its fate remains uncertain.[94]

In terms of data localisation issues, the unfolding transatlantic discussion seems to focus on exceptions complementary to Article XIV of the GATS. The US appears to insist on a wider 'national security' exception by providing similar exceptions to those presented in the TPP chapter, and follows the TPP definition of 'legitimate public policy objective'. Moreover, it seems that the US would like to extend this carve-out of data localisation rules to financial services – as in the TPP. The EU, meanwhile, insists on sticking to the GATS text. The Committee on Civil Liberties, Justice and Home Affairs (LIBE committee), in its opinion on the TTIP issued in 2015, also emphasised that there was a need for a comprehensive and unambiguous horizontal self-standing provision based on Article XIV of the GATS that fully exempts the existing and future legal framework for the protection of personal data from the scope of the agreement.[95]

TISA

The TiSA is currently being negotiated by 23 members of the WTO, including the EU. Together, the participating countries account for 70% of world trade in services. The talks started formally in March 2013, with participants agreeing on a basic text in September 2013. By the end of 2013 most participants had indicated which of their services markets they were prepared to open, and to what extent. By November 2016, 21 negotiation rounds had taken place.

93 Office of the US Trade Representative, 'Letter from Ambassador Demetrios Marantis, Acting US Trade Representative, to Congress', 20 March 2013, https://ustr.gov/sites/default/files/03202013%20TTIP%20Notification%20Letter.PDF, accessed 13 August 2017.

94 European Commission, 'European Commission launches EU–US Privacy Shield: Stronger protection for transatlantic data flows', Press Release, 12 July 2016, http://europa.eu/rapid/press-release_IP-16-2461_en.htm, accessed 7 August 2017.

95 European Parliament, Committee on Civil Liberties, Justice and Home Affairs, 'Draft opinion of the Committee on Civil Liberties, Justice and Home Affairs for the Committee on International Trade on recommendations to the European Commission on the negotiations for the Transatlantic Trade and Investment Partnership (TTIP)', 2014/2228(INI), 6 January 2015, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fNONSGML%2bCOMPARL%2bPE-546.558%2b01%2bDOC%2bPDF%2bV0%2f%2fEN, accessed 8 August 2017.

As in the case of the TTIP, negotiations are now on hold and are expected to resume when the political context allows. Formal discussions on data flows have not started yet, but several countries involved in TiSA, including the US, insist the agreement will crumble if there is no guarantee that data can travel between trade partners. Both the US and the EU are mandated to negotiate data flows within TiSA.[96] Yet the media have reported that the European Commission (in particular the Directorate-General for Justice and Consumers) has proposed a compromise position under which the new GDPR could never be challenged by the TiSA.[97] Such an exception could open the door to similar reactions from other countries, which could make a comparable claim in relation to their policies. At the time of writing, the agreement was still in limbo and the commission had not yet sent a proposal to member states for approval.

EU Free Flow of Data Initiative

In a communication published at the beginning of 2017, the European Commission followed up on its announcement, under the Digital Single Market strategy, that it intended to tackle restrictions on the free movement of data within the EU.[98] The communication states that free flow of data is essential for a well-functioning and dynamic data economy and that data localisation measures are effectively reintroducing 'digital border controls'.

The GDPR bans restrictions on the free movement of personal data within the EU where these relate to the protection of personal data. However, restrictions based on considerations other than the protection of personal data, eg, under taxation or accounting laws, are not covered by the GDPR. Moreover, non-personal data also remains outside the scope of the GDPR and can concern, for instance, non-personal machine-generated data.

96 The EU TiSA mandate states in that 'the negotiation should aim at including *inter alia* regulatory disciplines concerning ... cross-border data transfers'. See Council of the European Union, 'Draft Directives for the Negotiation of a Plurilateral Agreement on Trade in Services, Declassification of Document: 6891/13 ADD 1 Restreint UE/EU Restricted dated: 8 March 2013', Brussels, 10 March 2015, http://data.consilium.europa.eu/doc/document/ST-6891-2013-ADD-1-DCL-1/en/pdf, accessed 5 August 2017. The TPA also foresees language on data flows and data storage: 'Aside from ensuring that governments refrain from enacting measures impeding digital trade in goods and services, the proposed TPA-2015 extends that commitment to refrain governments from enacting measures impeding to cross-border data flows, data processing, and data storage.' See Fergusson IF & CM Davis, 'Trade Promotion Authority (TPA): Frequently Asked Questions', Congressional Research Service, 2 July 2015, https://fas.org/sgp/crs/misc/R43491.pdf, accessed 23 August 2017.

97 Stupp C, 'European Commission paralysed over data flows in TiSA trade deal', Euractiv, 10 October 2016, https://www.euractiv.com/section/trade-society/news/european-commission-paralysed-over-data-flows-in-tisa-trade-deal/, accessed 7 August 2017.

98 European Commission, 'Communication on Building a European Data Economy', 10 January 2017, https://ec.europa.eu/digital-single-market/en/news/communication-building-european-data-economy, accessed 14 July 2017.

The 'Communication on Building a European Data Economy' aims to fill this gap and prevent member states from imposing any restrictions on movement of data intra-EU when they are not necessary and proportionate to achieving an overriding objective of general interest, such as public security. According to the communication,

> any Member State action affecting data storage or processing should be guided by a 'principle of free movement of data within the EU', as a corollary of their obligations under the free movement of services and the free establishment provisions of the Treaty and relevant secondary legislation.[99]

The European Commission committed to:

- enter into structured dialogues with member states and other stakeholders on the justifications for and proportionality of data location measures currently implemented by member states; and
- where needed, launch infringement proceedings to address unjustified or disproportionate data location measures, and, if necessary, take further initiatives on the free flow of data.

WTO JURISPRUDENCE[100]

During the Uruguay round, the Internet was still in its infancy. Current WTO rules are thus not designed to reflect the Internet's implications for international trade. However, until all relevant countries agree in bilateral and plurilateral agreements on new trade rules that account for digital trade, the existing WTO discipline remains crucial.

The WTO jurisprudence offers clear arguments against imposing barriers to cross-border data flows, although it does not refer explicitly to data localisation

The WTO jurisprudence offers clear arguments against imposing barriers to cross-border data flows, although it does not refer explicitly to data localisation. In particular, imposing data localisation measures might result in a failure to comply with the GATS commitments on market access and national treatment.

According to WTO jurisprudence, the GATS commitments cover all means of supplying services and technological evolutions in supplying services. Moreover, the GATS commitments cover all services necessarily falling within the scope of

99 *Ibid.*

100 The main source for this section is Crosby D, 'Analysis of Data Localization Measures under WTO Services Trade Rules and Commitments', E15 Initiative Policy Brief, March 2016, http://e15initiative.org/publications/analysis-of-data-localization-measures-under-wto-services-trade-rules-and-commitments/, accessed 13 July 2017.

the sectoral definition. In this sense, digital services commitments involve many different services, including the cross-border transfer of business and customer data. Measures that prohibit the transfer of data across borders can therefore be interpreted as a violation of the GATS commitments on market access and national treatment, unless certain exceptions apply.

Two cases are particularly relevant, and confirm that the GATS commitments cover all means of supplying services and technological evolutions in supplying services, demonstrating that the GATS rules do apply to digital trade.[101] In US–Gambling, the WTO Panel found that supply of a service through 'mode 1' (cross-border provision) includes all means of delivery, including electronic means. It specifies that this assumption is 'in line with the principle of "technological neutrality", which seems to be largely shared among WTO Members'.[102] In its report of April 2005, the Appellate Body upheld the panel's finding that: [103]

> [a prohibition on one, several or all means of delivery cross-border] is a 'limitation on the number of service suppliers in the form of numerical quotas' within the meaning of Article XVI:2(a) because it totally prevents the use by service suppliers of one, several or all means of delivery that are included in mode 1.

In the China–Publications and Audiovisual Products case, the panel found that the scope of China's commitment in its GATS Schedule on 'sound recording distribution services' extended to sound recordings distributed in non-physical form, through technologies such as the Internet.[104] The Appellate Body confirmed that 'the terms used in China's GATS Schedule ("sound recording" and "distribution") are sufficiently generic that what they apply to may change over time' and therefore also cover products delivered in digital forms.[105]

101 This is already an important achievement per se. In the late 1990s some were arguing that neither trade rules in goods nor those in services applied to electronic commerce, and that new rules might be needed to regulate it. Jurisprudence under the GATS has obviated that danger and most GATS-related dispute settlements have involved online or networked services.

102 WTO, Dispute Settlement, 'DS285: United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services' (hereafter US–Gambling), https://www.wto.org/english/tratop_e/dispu_e/cases_e/ds285_e.htm, accessed 26 February 2018.

103 WTO, Report of the Appellate Body, 'United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services', 7 April 2005, https://www.wto.org/english/tratop_e/dispu_e/cases_e/ds285_e.htm, accessed 11 March 2018.

104 WTO, Dispute Settlement, 'DS363: China – Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products', https://www.wto.org/english/tratop_e/dispu_e/cases_e/ds363_e.htm, accessed 26 February 2018.

105 WTO, 'Report of the Appellate Body, 'China – Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products - AB-2009-3', December 2009, https://www.wto.org/english/tratop_e/dispu_e/cases_e/ds363_e.htm, accessed 12 August 2017.

Considering therefore that the GATS rules do apply to digital trade, it is possible to make the argument that data localisation requirements are a violation of the GATS commitments.

The GATS includes two sets of rules. One set applies to all services unless subject to reservations. This includes the 'most favoured nation' commitment, among others. The second set applies to specific sectors where members have scheduled a commitment to liberalise their service market. This set includes national treatment and market access commitments. If one assumes full commitments on data services through mode 1, any measure that makes it impossible to freely transfer business and personal data cross-border represents a limitation falling under the market access commitment (Article XVI). Therefore, any data localisation measure that imposes a ban on transferring data across borders entails a violation of WTO commitments.

Moreover, again assuming commitments relating to the supply of services in a certain sector and the mode of supply, data localisation would constitute a violation of national treatment rules (Article XVII). In fact, data localisation measures (and, in particular, infrastructure requirements) would result in less favourable treatment of foreign suppliers, as they would be required to build new servers or use local suppliers, which gives a clear competitive advantage to national service suppliers. Therefore, in cases where a WTO member has made commitments regarding the supply of digital services through mode 1, data localisation should not be applied.

This is reinforced by the text of the GATS Annex on Telecommunications, which requires each member to ensure that, in every sector where it has made commitments,[106]

> service suppliers of any other Member may use public telecommunications transport networks and services for the movement of information within and across borders, including for intra-corporate communications of such service suppliers, and for access to information contained in databases or otherwise stored in machine-readable form in the territory of any Member.

Such obligations are subject to the general exceptions presented in Article XIV of the GATS (Annex 2), which include issues related to national security, data privacy, fraud and safety. Yet the article makes it clear that such exceptions should not be applied in a manner that constitutes 'arbitrary or unjustifiable discrimination between countries' or 'a disguised restriction on trade in services'.[107] The question here is thus whether less trade-restrictive options than data localisation can be used to achieve the objective of protecting the privacy of individuals. In other words, are data localisation measures 'necessary' to achieve the stated goal? Or are there 'reasonably available WTO-consistent alternatives' that respond better to members' GATS obligations?

106 WTO, 'Annex on Telecommunications', Article 5, https://www.wto.org/english/tratop_e/serv_e/12-tel_e.htm, accessed 12 August 2017.

107 GATS: General Agreement on Trade in Services, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1B, 1869 U.N.T.S. 183, 33 I.L.M. 1167 (1994) (hereafter GATS).

'Necessary' was defined in the Appellate Body Report in the US–Gambling dispute settlement case. In the report, the body stated that:[108]

> The requirement, under Article XIV(a), that a measure be 'necessary' –that is, that there be no 'reasonably available', WTO-consistent alternative – reflects the shared understanding of Members that substantive GATS obligations should not be deviated from lightly. An alternative measure may be found not to be 'reasonably available', however, where it is merely theoretical in nature, for instance, where the responding Member is not capable of taking it, or where the measure imposes an undue burden on that Member, such as prohibitive costs or substantial technical difficulties. Moreover, a 'reasonably available' alternative measure must be a measure that would preserve for the responding Member its right to achieve its desired level of protection with respect to the objective pursued under paragraph (a) of Article XIV.

In this case, a member invoking the exception 'bears the burden of demonstrating that its measure, found to be WTO-inconsistent, satisfies the requirements of the invoked defense'.[109]

OPTIONS FOR SOUTH AFRICA

The challenge that most democratic economies face is how to enable data to flow freely while making sure that it remains private and protected. As shown in the section on data flow regimes in the BRICS economies, the BRICS countries approach the issue of cross-border data flows differently. China and Russia view the Internet and control over data as an important strategic interest, owing to both geopolitical concerns and the need to maintain public order. Brazil and India, meanwhile, have mostly opted to allow data to flow freely, while implementing or considering certain restrictions – especially on government data.

Currently, South Africa belongs to the latter group of countries, while its data privacy policy also takes inspiration from the conditional flow regime in the EU's Directive 46/95. This solution has been adopted mainly by developing countries, and is partly justified by their interest in gaining easier access to the European market. Yet the implementation of a conditional flow regime in practice has little impact on the possibility of a country's being granted the status of adequacy by the EU.[110]

Overall, the EU's adequacy decisions are rarely granted, and their issuance depends on more than just the regulatory regime in the partner country. Even when a country's regime is regarded as adequate, the EU prioritises those countries considered especially important from a political or commercial perspective.

108 WTO, 2005, *op. cit.*

109 *Ibid.*

110 For detailed information on the process of granting adequacy decision, see European Commission, 'Data protection: Rules for the Protection of Personal Data Inside and Outside the EU', http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm, accessed 11 March 2018.

Currently, the only discussions on an adequacy decision are being held with Japan and the Republic of Korea.

The South African government has three options when it comes to regulating cross-border data flows and positioning itself in the international discussion on data flows:

- maintaining the status quo;
- further liberalising data flows; or
- imposing new restrictions on data flows.

Maintaining the status quo

South Africa could maintain the current conditional flow regime, and refrain from pursuing any additional policy to promote or restrict data flows. While this is not ideal for local businesses and consumers, given the costs associated with fulfilling the conditions enshrined in the POPI, the regime is quite common globally and multinational companies already have the frameworks to comply with it. On the other hand, small and medium companies in South Africa and neighbouring countries might find it costly to deal with this regulation, with a consequent impact on productivity and growth (as shown in the section on the cost of data localisation).

Further liberalising the flow of data

The second policy option is liberalisation of the movement of data. This could be pursued either by changing the regulatory regime or by negotiating the liberalisation of data flows within the context of FTAs or similar initiatives.

The first alternative is maintaining the current regulatory protections for data privacy and security while eliminating the conditions for processing data outside South Africa. Data protection would remain the same, with the difference that data could be processed anywhere by the company.[111] This is already the case in countries such as the US[112] and would eliminate the additional costs associated with fulfilling conditions. Given that the country is not a candidate for an adequacy decision by the European Commission, this regime change would not impact South African companies' current access to the European market.

111 The only issue that might arise is that the enforcement of such rules would not be as straightforward as when the company is physically located in South Africa. A discussion of this topic goes beyond the scope of this paper, but it is important to mention that it is always in the company's interest to respect the privacy and security of its customers' data, and that it does not have any incentives to violate the law of the country in which it is operating – unless there is a conflict of jurisdiction. For a discussion on conflicting jurisdiction of data, see Daskal J, 'The un-territoriality of data', *Yale Law Journal*, 125, 2, 2015, pp. 326–559.

112 The US does have some conditions in place for certain types of sensitive data.

The second alternative is liberalising data flows in the context of trade agreements or similar initiatives. South Africa could propose the liberalisation of data flows in the context of the Southern African Customs Union and SADC FTAs. This approach would be similar to the one taken by the European Commission in the context of the EU Free Flow of Data Initiative,[113] and would send a clear political signal that the country wants to position itself as the data processing hub of the region.

South Africa could propose the liberalisation of data flows in the context of the Southern African Customs Union and SADC FTAs

In addition, South Africa could engage in other plurilateral or multilateral discussions with the objective to promote further liberalisation of data flows among trading partners.

Imposing new restrictions on data flows

The third option for South Africa is to impose new restrictions on movement of data, including the requirement that companies build data centres in the country. The negative consequences of such a decision would be significant, and certain international companies might flee the country because of the additional costs.

In the short term, there would be benefits for a small set of local companies engaged in data processing, but the gains would be outweighed by the losses in productivity, investment, welfare and security of data for all companies operating in the country – as confirmed by the literature review presented above. In particular, local companies would lose access to (or pay more for) services that would enable them to fully exploit the benefits of the digital economy and extract the benefits of data produced locally.

Moreover, most restrictions on data flows would have a lasting impact on the country's Internet infrastructure, which would not be easily reversible.

WAY FORWARD: EMERGING LESSONS FOR DOMESTIC AND GLOBAL ECONOMIC POLICY DISCUSSIONS

There are many justifications for the growing number of restrictions on cross-border data flows. In some cases, there is a lack of understanding of how the digital economy works, and countries wrongly assume that these measures will ensure jobs and growth. This paper has hopefully shed light on this argument, and shown how restrictions on data flows impose significant costs on the economy.

113 See the section on data flow regimes for more information.

Most restrictions on data flows would have a lasting impact on the country's Internet infrastructure, which would not be easily reversible

In other cases, countries have been willing to sacrifice economic benefits in return for greater control over their citizens' data, in the name of public order. This is the most likely rationale behind the strict restrictions imposed by China and Russia. Importantly, the idea that China's data flow restrictions are somehow connected to the country's staggering growth in digital economy and e-commerce sales is a misleading oversimplification (as economists would say: correlation does not imply causation).

Chinese digital companies rely heavily on government investment in digital infrastructure, fiscal incentives, and one of the biggest and fastest growing internal markets in the world. If anything, restrictions on data flows have prevented local companies from exporting their services abroad, and China's competitiveness in digital services remains low compared with other emerging economies. For example, its share in the global export of ICT services is 3.9%, compared with 12.2% for India.[114] This has been a conscious choice by the government, which has renounced further economic gains in order to maintain control over information flowing in and out of the country.

When countries are not concerned about maintaining control over data flows for public order, liberalising data flows remains the best way to benefit from the digital economy. In the era of cloud computing and data analytics, any restriction on data flows creates significant costs when accessing foreign services, and can make it impossible for local firms to use efficient and secure online solutions to build new products and services.

When countries are not concerned about maintaining control over data flows for public order, liberalising data flows remains the best way to benefit from the digital economy

Responding to the current policy uncertainty by imposing restrictions on data flows risks being an emotional decision driven by a misunderstanding about trade in the digital era. Data flows are a crucial input for the creation of innovative products and services, and the requirement to use local data centres would send a signal that the country is not open for business. Moreover, such a decision would be hard to

114 Own calculations based on UNCTAD Statistics, http://unctadstat.unctad.org/, accessed 4 November 2017.

reverse, given the profound impact it would have on infrastructure and business conduct in the country.

Responding to the current policy uncertainty by imposing restrictions on data flows risks being an emotional decision driven by a misunderstanding about trade in the digital era

Given the rapid changes in data policies across the globe, coupled with the current climate of uncertainty, it is not advisable for South Africa to undergo swift regulatory changes to data flows – despite the economic gains it would derive from liberalising the data regime. Maintaining the current policy regime while promoting liberalisation of data flows at the regional level appears to be the most suitable policy option for the country. This would enable South Africa to position itself as a regional hub for data processing services, while maintaining current provisions on data privacy.

The country should also remain engaged in multilateral discussions on data flows. In this way South Africa could actively shape policy measures on data flows rather than being a passive recipient of decisions taken in other trade contexts.

At the same time, it is of critical importance for South Africa to implement the necessary cybersecurity and privacy policies to protect data. This could be done by investing in mentoring programmes to train and support local businesses to implement appropriate privacy and cybersecurity practices, while ensuring that these firms have access to the most efficient services globally.

The government should also consider investing in digital skills and training. Other policy areas to consider are investment in quality infrastructure to ensure good and affordable Internet connectivity, and support of digital start-ups through incubators and accelerator programmes. Collaboration and open discussion with businesses and consumers' representatives should inform the policy dialogue, ensuring that their interests are reflected in the policy framework.

By doing so, South Africa can position itself as a forward-looking actor in the digital arena and fully exploit the opportunities offered by the digital economy.

ANNEX I LIST OF DATA LOCALISATION MEASURES[a]

COUNTRY	ACT OR PRACTICE	DESCRIPTION
Argentina	Law No. 25326 (Data Protection Act) Regulatory Decree No. 1558/2001	Section 12 of the Data Protection Act of Argentina (Law 25326) 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. 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.
Australia	Personally Controlled Electronic Health Record Act of 2012, Section 77	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 it does not include 'information in relation to a consumer' or 'identifying information of an individual or entity'.
Australia	Federal Privacy Act 1988 as amended by the Privacy Amendment (Enhancing Privacy Protection) Act 2012	Under the Federal Privacy Act, before an organisation 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 organisation.
Brunei	Local storage requirement	Brunei laws require that data generated within the country be stored only in servers within the country.

Canada	Personal Information International Disclosure Protection Act, S.N.S. 2006, c. 3, s. 5(1)	Nova Scotia requires that personal information held by a public body (primary/secondary schools, universities, hospitals, government-owned utilities and public agencies) must be stored or accessed only in Canada. 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'.
Canada	Freedom of Information and Protection of Privacy Act, R.S.B.C. 1996, c. 165, s. 30.1	British Columbia requires that personal information held by a public body (primary/secondary schools, universities, hospitals, government-owned utilities and public agencies) must be stored or accessed only in Canada. 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 information and has consented, in the prescribed manner, to it being stored in or accessed from, as applicable, another jurisdiction'.
Canada	Canadian Federal Law Personal Information Protection and Electronic Documents Act	According to the Canadian Federal Law Personal Information Protection and Electronic Documents Act, consent is not necessary for transfer to a third country, as the 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.
Canada	Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information	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'.
Canada	Freedom of Information and Protection of Privacy Act	Alberta's Freedom of Information and Protection of Privacy Act permits the disclosure of personal information controlled by a public body in response to a 'subpoena, warrant or order' only if issued by a court with 'jurisdiction in Alberta'.
China	Notice to Urge Banking Financial Institutions to Protect Personal Financial Information	The Notice to Urge Banking Financial Institutions to Protect Personal Financial Information states that personal information collected by commercial banks must be stored, handled and analysed within the territory of China and such personal information cannot be transferred overseas.

China	Administrative Measures for Population Health Information (For Trial Implementation)	Population health information needs to be stored and processed within China. In addition, storage is not allowed overseas.
China	Law of the People's Republic of China on Guarding State Secrets	The transfer abroad of data containing state secrets is prohibited.
China	Interim Measures for the Administration of Online Taxi Booking Business Operations and Services	China instituted a licensing system for online taxi companies that requires them to host user data on Chinese servers.
China	Data localisation requirement	China's data residency laws stipulate that companies can store the data they collect only on servers in country.
China	Map Management Regulations	Online maps are required to set up their server inside the country and must acquire an official certificate.
China	Administrative Regulations for Online Publishing Services ('Online Publishing Regulations')	Strict guidelines on 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 its 'necessary technical equipment, related servers and storage devices' in China.
China	Cybersecurity Law	The Cybersecurity Law requires, among others, that the personal information of Chinese citizens and 'important data' collected by 'key information infrastructure operators' (KIIOs) be kept within the borders of China. If KIIOs need to transfer this data outside of China for business reasons, security assessments must be conducted. The definition of KIIOs remains to be finalised.
China	Guidelines for Personal Information Protection Within Public and Commercial Services Information Systems	Article 5.4.5 of the Guidelines for Personal Information Protection Within Public and Commercial Services Information Systems prohibits the transfer of personal data abroad without the express consent of the data subject, government permission or explicit regulatory approval 'absent the 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.

Colombia	Law 1581 of 2012 (as regulated by Decree 1377 of 2013) Law 1266 of 2008 (as regulated by decrees 2952 of 2010 and 1727 of 2009)	Pursuant to Law 1266 of 2008, personal data may not be transferred outside of Colombia to countries that do not comply with adequate standards for data protection. This restriction does not apply in the following cases: • when there is express authorisation by the data subject; • when the information relates to medical data as required for reasons of health and public hygiene; • for banking operations; and • for operations carried out in the context of international conventions that Colombia has ratified.
EU	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)	The General Data Protection Regulation (GDPR) is set to replace Data Protection Directive 95/46/ec effective 25 May 2018. The GDPR permits personal data transfers to a third country or international organisation subject to compliance with set conditions. Similar to the directive, the GDPR allows for data transfers to countries whose legal regime is deemed by the European Commission to provide an 'adequate' level of personal data protection. Currently, 12 jurisdictions have been deemed to have an adequate level of protection: Andorra, Argentina, Canada, the Faroe Islands, Guernsey, Jersey, the Isle of Man, Israel, New Zealand, Switzerland and Uruguay. In addition, the EU/US Privacy Shield acts as a self-certification system open to certain US companies for data protection compliance. In the absence of an adequacy decision, however, transfers are also allowed outside non-EU states under certain circumstances, such as by use of standard contractual clauses or binding corporate rules (BCRs), or with the explicit consent of the data subject. Derogations are also permitted under limited additional circumstances.
Belgium	Companies Code	Article 463 of the Companies Code requires that the company register of shareholders and register of bonds be kept at the registered office of the company. Since 2005 it has been possible to keep these registers in electronic format, as long as they are accessible at the registered office of the company.
Belgium	VAT Code, Article 60	With respect to value added tax (VAT), invoices received and copies of invoices issued by taxpayers must be stored in Belgium or in another EU member state under certain conditions. Invoices must be stored in either electronic or paper format (Article 60, § 3 of the VAT Code).
Belgium	Income Tax Code, Article 315	With respect to income tax, except when an exemption is granted by the administration, books and documents must be kept in the office, agency, branch or other professional or private premises of the taxpayer where they have been stored, prepared or received, at the disposal of the tax authority.

Bulgaria	Gambling Act	In Bulgaria, an applicant for a gaming licence 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 central computer system of the organiser are located within the EEA or in Switzerland.
Denmark	Consolidated Act No. 648 of 15 June 2006 (Bookkeeping Act)	According to the Bookkeeping Act (Section 12), financial records must be stored in Denmark or the Nordic countries. This applies to both physical appendixes and digital data. Hence, if financial records are stored on a server located outside Denmark a complete copy must be kept in Denmark.
Denmark	Consolidated Act No. 1035 of 21 August 2007 (Audit Act)	According to the Audit Act (Section 45), the financial records of 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 a copy must be kept on a server in Denmark or on paper.
Denmark	Consolidated Act No. 528 of 15 June 2000 as changed by Act No. 201 of 22 March 2001 (Executive Order on Security)	Since 2011 the Danish Data Protection authority has ruled in several cases against processing local authorities' data in third countries without using standard contractual clauses. This is the result of a strict interpretation of the European Directive 95/46/EC. Therefore, services such as Dropbox, Google Apps and Microsoft's Office 365 cannot be used by local authorities unless they have signed an agreement with the processor with standard contractual clauses.
Finland	Accounting Act (1336/1997)	The Accounting Act requires that a copy of accounting records be kept in Finland. Alternatively, the records can be stored in another EU country if a real-time connection to the data is guaranteed.
France	Ministerial Circular from 5 April 2016, Note d'information du 5 avril 2016 relative à l'informatique en nuage (cloud computing)	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 public service data thus has to be considered as archival and therefore stored and processed in France.
Germany	Act on Value Added Tax, Section 14b (Umsatzsteuergesetz, UStG)	The Act on VAT states that invoices must be stored within the country, including when stored electronically. Alternatively, in case of electronic storage, they may be stored within the territory of the EU if full online access and downloading capacity 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.

Germany	Tax Code, Section 146(2) 1 (Abgabenordnung, AO)	Under the Tax Code, all persons and companies liable to pay taxes and that are obliged to keep books and records must keep those records in Germany. There are some exceptions for multinational companies.
Germany	German Commercial Code, Section 257 No. 1 and 4 (Handelsgesetzbuch § 257)	According to the German Commercial Code, accounting documents and business letters must be stored in Germany.
Germany	German Telecommunications Act, as amended in December 2015	Under the Directive on Data Retention, operators were required to retain certain categories of traffic and location data (excluding the contents 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. On 8 April 2014 the Court of Justice of the European Union declared the directive invalid. However, not all national laws that implemented the directive have been overturned. In 2010 the German Constitutional Court found that the implementation of the Directive on Data Retention was unconstitutional. In October 2015 a new data retention law was passed, entering into force in 2017. The law provides that telecommunications providers must retain data such as phone numbers, the time and place of communications (except for emails), and IP addresses for either four or 10 weeks. The data is to be stored in servers located within Germany (§113b).
Greece	National Law 3917/2011	In Greece, 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 data on 'traffic and localisation' stay 'within the borders of the Hellenic territory'. The law is still in force.
Italy	Presidential Decree No. 633 of 1972	Article 39 of Presidential Decree No. 633 of 1972 states that electronic archives related to accounting data on VAT declarations may be kept in a foreign country only if a convention has been concluded between Italy and the receiving country governing the exchange of information in the field of direct taxation. This limitation does not apply intra-EU.
Luxembourg	Circular CSSF 12/552, as amended by circulars CSSF 13/563 and CSSF 14/597	According to Circular CSFF 12/552, financial institutions in Luxembourg are required to process their data within the country. Processing abroad is permitted in exceptional cases for an entity of the group to which the institution belongs or with explicit consent.

The Netherlands	Public Records Act	Localisation requirements apply to public records that have to be stored in archives in specific locations in the Netherlands. This applies to both paper and electronic records.
Poland	Polish Gambling Act	According to the Polish Gambling Act, any entity organising gambling activities is obliged to archive in real time all data exchanged between such entity and the users in an archive device located in Poland. Another restriction is the requirement that the equipment (servers) for processing and storing information and data on bets and their participants must be installed and kept on the territory of a member state of the EU or the European Free Trade Association.
Portugal	Data Protection Law	In Portugal, the Portuguese Data Protection Authority (DPA) must be notified of all data transfers outside the EU and, except when directed to whitelisted countries or when using model contracts, these have to be authorised by the relevant commission. On 10 November 2015 the Portuguese DPA also issued specific guidelines on Intra-Group Agreements (IGA) involving transfers of personal data to non-EEA countries. Such transfers depend on prior authorisation from the DPA for the purposes of assessing if the IGAs contain sufficient guarantees that the personal data transferred will benefit from the same level of protection as in EEA countries.
Romania	Law No. 124 from May 2015, regarding the approval of Government Emergency Ordinance No. 92/2014 regulating fiscal measures and modification of laws	In Romania, the game server must store all data related to the provision of remote gambling services, including the records and identification of players, the bets placed and the winnings paid out. Information must be stored using data storage equipment (mirror servers) situated in Romanian territory.
Romania	Law on the Protection of Individuals with regard to the Processing of Personal Data and the Free Movement of Such Data (Data Protection Law)	In Romania, any transfer of personal data to any state requires prior notification to the National Supervisory Authority for Personal Data Processing. Any transfer of personal data to a recipient state not offering an adequate level of protection needs prior approval.
Slovenia	Slovenian Personal Data Protection Act	In Slovenia, transfers of personal data to non-EEA and non-whitelist countries require the approval of the commissioner. The approval is issued if the commissioner establishes that a sufficient level of protection is ensured for the transfer of personal data.

Spain	Organic Law relating to Personal Data Protection	In Spain, cross-border data flows subject to model contracts or binding corporate rules require prior authorisation from the director of the Spanish Data Protection Authority.
Sweden	Swedish Accounting Act (Bokföringslag [1999:1078])	In Sweden, documents such as a company's annual reports, balance sheets and financial reports must be physically stored in the country for a period of seven years.
Sweden	Local storage requirement	In relation to specific government authorities, there are certain provisions that might require that data processed by the authority be held within Sweden or within the authority. This might affect the supply of cloud computing to public authorities.
Sweden	Local storage requirement	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 service providers are *de facto* required to maintain all their records within Swedish jurisdiction.
UK	Companies Act 2006, Art. 388	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'.
Iceland	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)	As member of the EEA, Iceland follows the same data protection rules as the 28 European member states. The General Data Protection Regulation (GDPR) is set to replace Data Protection Directive 95/46/ec effective 25 May 2018. The GDPR permits personal data transfers to a third country or international organisation subject to compliance with set conditions. Similar to the directive, the GDPR allows for data transfers to countries whose legal regime is deemed by the European Commission to provide an 'adequate' level of personal data protection. Currently, 12 jurisdictions have been deemed to have an adequate level of protection: Andorra, Argentina, Canada, the Faroe Islands, Guernsey, Jersey, the Isle of Man, Israel, New Zealand, Switzerland and Uruguay. In addition, the EU/US Privacy Shield acts as a self-certification system open to certain US companies for data protection compliance. In the absence of an adequacy decision, however, transfers are also allowed outside non-EU states under certain circumstances, such as by use of standard contractual clauses or binding corporate rules (BCRs), or with the explicit consent of the data subject. Derogations are also permitted under limited additional circumstances.

India	Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules	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 a 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 a transfer has been consented to by the provider of information.
India	National Data Sharing and Accessibility Policy Public Records Act, No. 69 of 1993	In 2012 India enacted the National Data Sharing and Accessibility Policy, which effectively means that government data (data owned by government agencies and/or collected using public funds) must be stored in local data centres. 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 states: '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.'
India	Guidelines for Government Departments on Contractual Terms Related to Cloud Services	In 2015 India's Ministry of Electronics and Information Technology issued guidelines for a cloud computing empanelment process under which cloud computing service providers may be provisionally accredited as eligible for government procurements of cloud services. However, the guidelines require that such providers store all data in India to qualify for the accreditation.
Indonesia	Government Regulation No. 82 of 2012 regarding the Provision of Electronic System and Transaction (Regulation 82)	Regulation 82 states that storing personal data and performing a transaction with the data of Indonesian nationals outside the Indonesian jurisdiction is restricted. This requirement appears to apply particularly to the personal and transaction data of Indonesian nationals that is used within Indonesia and/or related to Indonesian nationals. 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 Centres. The unclear and possibly all-encompassing definition of public services gave rise to concerns when a spokesperson was quoted saying that '[the draft] covers any institution that provides information technology-based services'. Data carriers covered by this provision, therefore, would include a wide range of actors such as cloud providers, foreign banks and mobile phone providers.

Indonesia	Law No. 11 of 2008 regarding Electronic Information and Transaction Government Regulation No. 82 of 2012 regarding the Provision of Electronic System and Transaction (Regulation 82) Draft Regulation with Technical Guidelines for Data Centres	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 came into force on 15 October 2012. Regulation 82 requires 'electronic systems operators for public services' to set up a data centre and a 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 Centres. The unclear and possibly all-encompassing definition of public services gave rise to concerns when a spokesperson was quoted saying that '[the draft] covers any institution that provides information technology-based services'. Data carriers covered by this provision, therefore, would include a wide range of actors such as cloud providers, foreign banks and mobile phone providers.
Indonesia	Circular Letter of Bank Indonesia No. 16/11/DKSP Year 2014 regarding E-money Operations	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 e-money operators to locate data centres and data recovery centres within the territory of Indonesia.
Indonesia	Government Regulation No. 82 of 2012 regarding the Provision of Electronic System and Transaction (Regulation 82)	According to Regulation 82, there are some situations where both parties have an agreement that includes clauses relating to data transferring activities. In these situations, it is thought that this agreement is sufficient as a ground for data transferring activities. Yet obtaining consent would complement the requirement to minimise future complaints from the data subject.
Israel	Privacy Protection Act, 5741-1981 Privacy Protection Regulations (Transfer of Data to Databases Outside of Israel), 2001	The Privacy Protection Regulations of 2001 permit transfers to: EU member states; other signatories of Council of Europe Convention 108; and a country 'which receives data from Member States of the European Community, under the same terms of acceptance'. Transfers to other countries are permitted: • subject to data subject consent; • from an Israeli corporate parent to a foreign subsidiary; or • provided the data importer enters into a binding agreement with the data exporter to comply with Israeli legal standards concerning the storage and use of data.

Japan	Act on the Protection of Personal Information (Act No. 57 of 2003, or APPI)	The Act on the Protection of Personal Information (APPI) did not originally restrict the transfer of personal information to foreign countries. Recent amendments that took effect in May 2017 added cross-border transfer restrictions. The amended APPI prescribes three types of legitimate transfers of personal information to a third party in a foreign country: (1) transfers to a country that the Personal Information Protection Commission has designated as having an acceptable level of data protection; (2) transfers to a third party in a foreign country in circumstances in which actions have been taken to ensure the same level of data protection as in Japan (such as entering into a data transfer agreement imposing obligations on the transferee meeting the requirements of the APPI); or (3) transfers with the data subject's consent.
Korea, Republic of	Act on the Establishment, Management, etc. of Spatial Data, Article 16	Korea imposes a prohibition on storing 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 local competitors are able to provide several services (such as turn-by-turn driving/walking instructions, live traffic updates, interior building maps) that international service providers cannot.
Korea, Republic of	Personal Information Protection Act, Article 17 (3)	The Personal Information Protection Act requires companies to obtain consent from data subjects prior to exporting their personal data.
Korea, Republic of	Act on Promotion of Information and Communications Network Utilisation (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.

Korea, Republic of	Financial Holding Company Act (FHCA)	Despite provisions in its FTAs with the EU and US to allow sending financial data 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 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 standardised outsourcing contract form (thus permitting customised contracts provided they include certain obligatory terms). Such revisions were implemented in July 2015. Certain conditions for processing abroad still apply.
Malaysia	Personal Data Protection Act 2010	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 entered into either 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 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 it officially entered into force in November 2013, the PDPA has not yet been enforced.

Mexico	Federal Law for the Protection of Personal Data in the Possession of Private Parties	According to the Federal Law for the Protection of Personal Data in the Possession of Private Parties, domestic and international transfers need the consent of the individual. Additionally, the data controller must provide third parties with the privacy notice that was sent to and consented to by the individual. Consent is not required for international transfer: • if transfer is intra-group; • if it results from a contract executed or to be executed in the interest of the data owner between the data controller and a third party; or • in a few other circumstances.
New Zealand	Inland Revenue Acts	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.
New Zealand	Privacy Act of 1993	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 has 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.
Nigeria	Guidelines on Nigerian content development in information and communications technology	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 is that 'Data and Information Management Firms' must host government data locally within the country and shall not for any reason host any government data outside the country without the express approval of the NITDA and the secretary of the federal government. Another requirement is that all ICT companies must host their subscriber and consumer data locally.
Nigeria	Guidelines on Point-of-Sale Card Acceptance Services	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.

Norway	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)	As member of the EEA, Norway follows the same data protection rules as the 28 European member states. The General Data Protection Regulation (GDPR) is set to replace Data Protection Directive 95/46/ec effective 25 May 2018. The GDPR permits personal data transfers to a third country or international organisation subject to compliance with set conditions. Similar to the directive, the GDPR allows for data transfers to countries whose legal regime is deemed by the European Commission to provide an 'adequate' level of personal data protection. Currently, 12 jurisdictions have been deemed to have an adequate level of protection: Andorra, Argentina, Canada, the Faroe Islands, Guernsey, Jersey, the Isle of Man, Israel, New Zealand, Switzerland and Uruguay. In addition, the EU/US Privacy Shield acts as a self-certification system open to certain US companies for data protection compliance. In the absence of an adequacy decision, however, transfers are also allowed outside non-EU states under certain circumstances, such as by use of standard contractual clauses or binding corporate rules (BCRs), or with the explicit consent of the data subject. Derogations are also permitted under limited additional circumstances.
Pakistan	Prohibition of data transfer	Although the transfer of data to third parties is not specifically regulated under the laws of Pakistan, data cannot be transferred to a country that is not recognised by Pakistan. Currently, the list of countries not recognised by Pakistan include Abkhazia, Armenia, Israel, Kosovo, Nagorno-Karabakh, Northern Cyprus, Sahrawi Arab Democratic Republic, Somaliland, South Ossetia, Taiwan and Transnistria. This list may change from time to time. Furthermore, data can only be transferred to India if such a transfer can be justified by the transferor.
Peru	Law No. 29733 (Personal Data Protection Law)	In the case of cross-border transfers, the data holder generally must refrain from transferring personal data if the destination country does not offer 'adequate protection levels', which are equivalent to those offered by the Personal Data Protection Law or in international standards. If the destination country fails to offer adequate protection levels, the controller must guarantee that the treatment of personal data meets such requirements (for example, via a written agreement). This guarantee is not necessary if the owner of the personal data has given prior, informed, express and unequivocal consent to the transfer, or if other exceptions apply. Moreover, any cross-border data transfers must be reported to the Peruvian Data Protection Authority.

The Philippines	Guidelines on Outsourcing Resolution No. 2115 of 2015, Amendments to the Manual of Regulations for Banks and the Manual of Regulations for Non-Bank Financial Institutions on the guidelines on outsourcing	According to Circular No. 899, offshore outsourcing of a bank's domestic operations is permitted only when the service provider operates in jurisdictions that uphold confidentiality. When the service provider is located in other countries, the bank should take into account and closely monitor, on continuing basis, government policies and other conditions in the countries where the service provider is based during a risk assessment process. The Bangko Sentral (Central Bank of Philippines) examiners shall be given access to the service provider and those relating to the outsourced domestic operations of the bank. Such access may be fulfilled by on-site examination through coordination with host authorities, if necessary.
Russian Federation	Federal Law No. 152-FZ 'On Personal Data' (OPD Law) as amended in July 2014 by Federal Law No. 242-FZ 'On Amendments to Certain Legislative Acts of the Russian Federation for Clarification of Personal Data Processing in Information and Telecommunications Networks'	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 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 citizens of the Russian Federation are 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 servers from abroad, and does not impose any special restrictions on cross-border data transfers or duplication of personal data. Online websites that violate the prohibition could be placed on the Roskomnadzor blacklist.
Russian Federation	Federal Law No. 161-FZ 'On the National Payment System' dated June 2011 (NPS Law) as amended in October 2014 by Federal Law No. 319-FZ 'On Amendments to the Federal Law on the National Payment System and Certain Legislative Acts of the Russian Federation'	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 operator (National Payment Card System) by 31 March 2015. The amendments are reported to be a response to the international political sanctions that prohibited certain international payment systems (eg, Visa and MasterCard) from servicing payments on cards issued by sanctioned Russian banks.

Russian Federation	Federal Law No. 374 on Amending the Federal Law 'on Counterterrorism and Select Legislative Acts of the Russian Federation Concerning the Creation of Additional Measures Aimed at Countering Terrorism and Protecting Public Safety'	Federal Law No 374-FZ, signed in July 2016, requires local storage for a period of three years (with respect to telecom providers) or one year (with respect to Internet arrangers) of information confirming the *fact* of receipt, transmission, delivery and/or processing of voice data, text messages, pictures, sounds, video or other communications (ie, metadata reflecting these communications). In addition, local storage for a period of six months is required for the *contents* 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 comes into force in July 2018.
Russian Federation	Government Decree No. 758 of 31 July 2014 and No. 801 of 12 August 2014	The Russian Government has given instructions that require public Wi-Fi user identification. The government decrees require that: • ISPs should identify Internet users, by means of identity documents (such as passports); • ISPs should identify terminal equipment by determining the unique hardware identifier of the data network; and • all legal entities in Russia should provide ISPs with a monthly list of individuals who accessed 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 fines for non-compliance: • RUB 5,000–50,000 (approx. $60–140) for individual entrepreneurs; and • RUB 100,000–200,000 (approx. $1,400–2,600) for legal entities. The fines would be higher for repeating offenders.
Russian Federation	Federal Law No. 152-FZ 'On Personal Data' (OPD Law) of July 2006	According to the OPD Law, the transfer of data outside Russia does not require additional consent from the data subject only if the jurisdiction to which the personal data is transferred ensures adequate protection. Those jurisdictions are the parties to the Convention 108 and other countries approved by Roskomnadzor. Roskomnadzor's official list of countries includes Argentina, Australia, Canada, Israel, Mexico and New Zealand.

Singapore	Personal Data Protection Act	An organisation may only transfer personal data outside Singapore if it has taken appropriate steps to ensure that: • it will comply with Personal Data Protection Act (PDPA) obligations in respect of the transferred personal data while it remains in its possession or under its control; and • the recipient outside Singapore is bound by legally enforceable obligations to provide a standard of protection to the personal data transferred that is comparable to that under the PDPA. An organisation will be taken to have satisfied the second requirement if the individual consents to the transfer of personal data to the recipient in that country.
South Africa	Protection of Personal Information Act 4 of 2013	Consent is needed for data transfers to third countries. Otherwise, the transfer can happen if: • the third party is subject to a law, binding corporate rules or binding agreement that provide an adequate level of protection; • the transfer is necessary for the performance of a contract between the data subject and the responsible party, or • the transfer is necessary for the implementation of pre-contractual measures taken in response to the data subject's request.
Switzerland	Swiss Federal Protection Act	According to the Swiss Federal Protection Act, personal data may only be transferred to countries with legislation providing an adequate level of protection of personal data. These comprise EU member states, whitelisted countries (currently Andorra, Argentina, Canada, the Faroe Islands, Guernsey, Israel, the Isle of Man, Jersey, New Zealand, Switzerland and Uruguay) and the US for those companies or organisations that have self-certified themselves under the US–Swiss 'Safe Harbour' framework. If the recipient country does not have legislation providing an adequate level of data protection, one of the following conditions must be fulfilled: • the existence of a trans-border dataflow contract or other 'sufficient safeguards'; • sufficient binding corporate rules; • the data subject's consent; • the export of the personal data at issue is required for the conclusion or performance of a contract with the data subject; • the export of the personal data is in the public interest; • the export of the personal data is necessary to protect the life or physical integrity of the data subject; or • the data subject itself has made the personal data publicly available.

Taiwan	Personal Data Protection Act	The transfer of personal information to mainland China is prohibited.
Taiwan	Personal Data Protection Act (PDPA), Article 21	There is no consent requirement for transfer to third countries, but the data subject has to be notified in advance that his/her personal data is being transferred to another country. According to Article 21 of the Personal Data Protection Act, 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.
Taiwan	Regulations Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operation	The Financial Supervisory Commission established stringent rules for processing personal financial information offshore. On May 2014 the requirements that both local and foreign banks establish standalone onshore data centres were lifted.
Turkey	Payment Services and Electronic Money Institutions Law No. 6493	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'. It 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'.
Turkey	Data Protection Law No. 6698	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 required by law, and either: • sufficient protection exists in the transferee country, or • the data controller gives a written security undertaking and Turkey's Data Protection Board grants permission.
Turkey	Electronic Communications Act	The transfer of traffic and location data abroad is permitted with the data subjects' explicit consent.
Turkey	Regulation on Processing and Protection of Confidentiality of Personal Data in the Electronic Communication Sector	In August 2013 Turkey approved the Regulation on Processing and Protection of Confidentiality of Personal Data in the Electronic Communication Sector was approved and it took effect in January 2014. This regulation imposes strict conditions on transfers of personal data outside of Turkey by telecommunications providers in Turkey.

US	Network Security Agreements	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 US 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, Department of Homeland Security, Department of Justice, Department of Defense 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 US government agencies seek access to the massive amounts of data flowing through their networks, the companies have systems in place to provide it securely'.[b] 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.
Vietnam	Decree No. 72/2013/ND-CP of 15 July 2013, on the Management, Provision and Use of Internet Services and Online Information	Decree No. 72 entered into force in September 2013, and establishes local server requirements for online social networks, general information websites, mobile telecoms network-based content services and online gaming 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'.
Vietnam	Decree 90/2008/ ND-CP dated 13 August 2008 on anti-spam (Decree 90)	According to 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 that is operated from a server located in Vietnam.

a PE, DTE, Database, http://www.ecipe.org/dte/database, accessed 11 March 2018. The information is complemented with additional research based on new laws implemented recently in the 64 economies listed in the DTE database.

b *The Washington Post*, 'Agreements with private companies protect US access to cables' data for surveillance', 6 July 2013, https://www.washingtonpost.com/business/technology/agreements-with-private-companies-protect-us-access-to-cables-data-for-surveillance/2013/07/06/aa5d017a-df77-11e2-b2d4-ea6d8f477a01_story.html, accessed 11 March 2018.

GEGAFRICA

GLOBAL ECONOMIC GOVERNANCE