GEGAFRICA
GLOBAL ECONOMIC GOVERNANCE

POLICY BRIEFING | FEBRUARY 2018

# SOUTH AFRICA: OPTIONS TO REGULATE DATA FLOWS

MARTINA F FERRACANE[1]

## EXECUTIVE SUMMARY[2]

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 policy briefing provides clear economic arguments to support a regime of free data flow 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.

## 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.[3] Data flows are creating significant value for the global economy and exert a greater impact on growth than traditional goods flows.[4]

Despite these significant benefits, the concentration of certain digital activities in the hands of a few 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 policy briefing explores this phenomenon and clarifies why this assumption is often wrong. Restrictions to data flows – also 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 a 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.

## DATA FLOWS: REGULATORY REGIMES APPLIED WORLDWIDE

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.[5]

**Restrictions to data flows – also referred to as data localisation measures – are detrimental to the local economy and impose unnecessary costs on local businesses and consumers**

The first, and least restrictive, regime is when a 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.

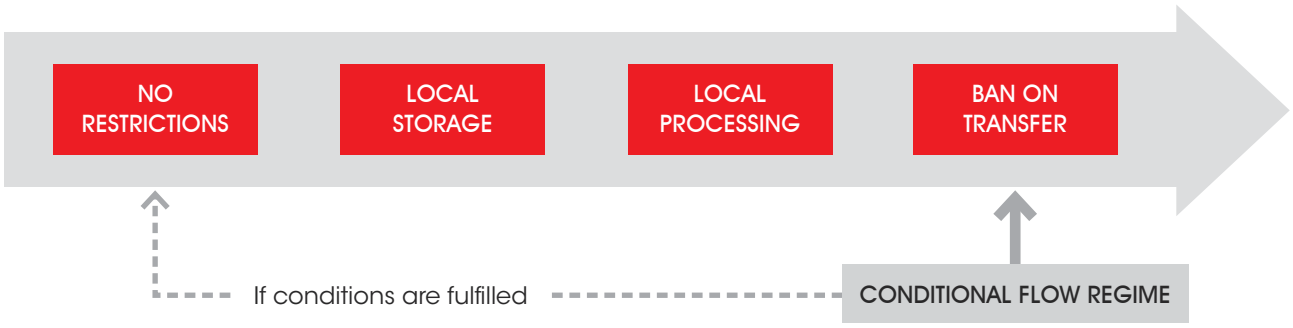
The second degree is when a country imposes a local storage requirement, where companies are required to store a copy of certain data within the country; the data can still be transferred and processed abroad. As long as a copy of the data remains within the national territory, the company can operate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

The third degree is the case of local processing. When a country imposes this requirement, companies have to 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.

The fourth, and most restrictive, degree is a ban on transfers of data abroad. Such a policy usually applies to specific sets of data considered especially sensitive, such as health or financial data. In this case, the company is not even allowed to send a copy of the data cross-border.

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 transfer.[6]

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




Source: Ferracane MF, 'Restrictions to Cross-Border Data Flows: A Taxonomy', ECIPE (European Centre for International Political Economy) Working Paper, 1, November 2017, http://ecipe.org/publications/restrictions-to-cross-border-data-flows-a-taxonomy/

## 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 but also globally.[7] 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 their national industry, but ultimately opted against such measures.[8] This is probably owing to the consideration that short-term gains from restricting data flows would be offset by losses in productivity, investment and ultimately growth (see below).

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

## THE COST 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.

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 higher costs in accessing foreign data processing services. A study from the Leviathan Security Group finds that in many countries that are considering 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.[9] Resources are therefore diverted from other investments that the company could make – including hiring new employees and buying new equipment.

Barriers to data flows also create delays and higher costs for companies wishing to access innovative goods and services that rely on cross-border data flows. 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.[10] In addition, building new business ideas that rely on other existing services worldwide also becomes more expensive, or even impossible.[11] The resultant delays and costs are borne by both local businesses and consumers. 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.

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

Measures imposing restrictions on data thus impact the productivity of firms not only in the digital sector but also in virtually any sector of the economy. In turn, the additional costs of processing data and accessing innovation have a trickle-down impact on the macroeconomic performance of those countries implementing data localisation rules.

The first comprehensive study that attempted to quantify the macroeconomic impact of data localisation was conducted by the European Centre for International Political Economy (ECIPE) in 2014.[12] ECIPE's study measures the impact of data localisation measures on gross domestic product (GDP), investment and consumer welfare, owing to higher prices and displaced domestic demand.

The estimated impact of proposed or enacted data restrictions on GDP is as follows: Brazil (-0.2%), China (-1.1%), the EU (-0.4%), India (-0.1%), Indonesia (-0.5%), the Republic of Korea (-0.4%) and Vietnam (-1.7%).[13] 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, almost 13% in China, and around 20% in South Korea and Brazil.

The costs to businesses and the economy as a whole are therefore substantial. At the same time, only a few local data processing companies benefit from these measures, and a small number of jobs are created. In fact, jobs associated with data centres have been decreasing sharply as data centres become more automated. Data centres contain expensive hardware that is often imported[14] and create only short-term construction work, while they employ relatively few full-time staff. In 2008, for example, Yahoo, Ask.com, Intuit and Microsoft hired a total of 180 workers for their facilities – an average of 45 workers per facility.[15] In 2015 media reports also showed that Apple's $2 billion global command centre in Mesa, Arizona would employ 150 full-time personnel, and result in between 300 and 500 construction and trade jobs.[16]

## OPTIONS FOR SOUTH AFRICA

The challenge that most of today's democratic economies face is how to enable data to flow freely while making sure it remains private and protected. 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.

Currently, South Africa belongs to the latter group of countries. Its data privacy policy takes inspiration from the conditional flow regime in the EU's Directive 46/95. This solution has been adopted by several countries, and is partly justified by their interest in gaining easier access to the European market. Yet in practice the implementation of a conditional flow regime is not enough for a country to be granted the status of adequacy by the EU.[17]

Overall, the EU's adequacy decisions are rarely granted, and their issuance is related to 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. 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 country's Protection of Personal Information Act, 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 the consequent impact on productivity and growth.

### 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 free trade agreements or similar initiatives.

The first alternative would consist of maintaining the current regulatory protections for data privacy and security, while eliminating the conditions for data processing outside South Africa. Data protection would remain the same, with the difference that data could be processed anywhere by the company. This is already the case in countries such as the US,[18] 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 change in the regime would not impact South African companies' current access to the European market.

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 free trade agreements. This approach would be similar to the one taken by the European Commission in the context of the EU Free Flow of Data Initiative, and would give a clear political signal that the country wants to position itself as the data processing hub of the region.

**Liberalising data flows in the context of trade agreements or similar initiatives would give a clear political signal that the country wants to position itself as the data processing hub of the region**

In addition, South Africa could consider engaging in other plurilateral or multilateral discussions with the objective to promote further liberalisation of data flows.

### 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. 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 various 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. However, as this brief has shown, restrictions on data flows impose significant costs on the economy.

In other cases, certain 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 its 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 information and communications services is 3.9%, compared with 12.2% for India.[19] 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.

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.

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

**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**

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.

**It is of critical importance for South Africa to implement the necessary cybersecurity and privacy policies to protect data**

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 forward-looking actor in the digital arena and fully exploit the opportunities offered by the digital economy.

## ENDNOTES

1 Martina F Ferracane is a PhD student in Law and Economics at Hamburg University and a Research Associate at the European Centre for International Political Economy (ECIPE), researching digital trade issues and data flows.

2 This policy brief is based on the forthcoming GEGAfrica Discussion Paper, 'South Africa and Data Flows: How to Fully Exploit the Potential of the Digital Economy'. For a detailed analysis of the issue, please consult the full paper.

3 Baldwin R, *The Great Convergence: Information Technology and the New Globalization*. Cambridge, MA: Belknap Press (Harvard University Press), 2017.

4 McKinsey estimates that data flows contributed about $2.8 trillion to the global economy in 2014 alone. See MGI (McKinsey Global Institute), 'Digital globalization: The new era of global flows', February 2016, http://www.mckinsey.com/business-functions/

mckinseydigital/our-insights/digital-globalization-the-new-era-of-global-flows, accessed 4 August 2017.

5 It is important to note that countries can apply different types of restrictions to different sectors and data. One country may thus have several levels of restrictions.

6 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 which might de facto result in a conditional flow regime.

7 See ECIPE (European Centre for International Political Economy), 'Digital trade estimates database', www.ecipe.org/dte/database, accessed 2 August 2017; Ferracane MF & E Van der Marel, 'Digital Trade Estimates Report 2017', ECIPE (forthcoming).

8 India does impose certain restrictions in the public sector. See Ferracane MF & E Van der Marel, *op. cit*.

9 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.

10 Cory N, *Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?*, ITIF (Information 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 1 August 2017.

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

12 Bauer M *et al*., 'The Costs of Data Localisation: Friendly Fire on Economic Recovery', ECIPE Occassional Paper, 3/2014, March 2014, http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf, accessed 13 August 2017

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

14 Cory N, *op. cit*.

15 O Hara 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 20 August 2017; 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 30 July 2017.

16 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 7 August 2017.

17 For detailed information on the process of granting an adequacy decision, see European Commission, 'Data protection', http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm, accessed 10 August 2017.

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

19 Own calculations based on UN Conference on Trade and Development (UNCTAD) Statistics. See UNCTAD, 'Product concentration index, 2016', http://unctadstat.unctad.org/, accessed 17 November 2017.

GEGAfrica has been funded by UK aid from the UK government; however, the views expressed do not necessarily reflect the UK government's official policies.


GEGAFRICA
GLOBAL ECONOMIC GOVERNANCE