POLICY BRIEF 03

MANDELA INSTITUTE

DATA PROTECTION AND DATA LOCALISATION IN KENYA:

POTENTIAL ECONOMIC IMPACT AND EFFECT ON KENYA'S COMMITMENTS IN VARIOUS REGIONAL TREATY FRAMEWORKS

Malcolm Kijirah *and* Elaine Wangari Thuo

MANDELA INSTITUTE, SCHOOL OF LAW, UNIVERSITY OF THE WITWATERSRAND

UNIVERSITY OF THE WITWATERSRAND, JOHANNESBURG

CONTENTS

ABSTRACT

Data localisation is a form of restriction of data flows across national borders. It broadly requires that personal data is stored within the national borders of the respective data subject's country. This trend has had great uptake recently, with the rise of national data protection laws in many African countries.

Various countries have justified the need to control data flows through a multitude of reasons including national security, cybersecurity, personal data protection and economic protectionism, among others. As much as some countries have strongly embedded this requirement in their laws, others view it as detrimental to trade and the economy. Many African countries have data protection laws modelled in line with the General Data Protection Regulation (GDPR) in the European Union. This, arguably, supports a conclusion that these measures are implemented so as to enable a favourable environment to conduct business with countries that have adopted similar data protection laws in line with the GDPR. In addition, various regional laws affect the regulatory framework for data protection. For example, trade blocks regulatory frameworks, such as The African Union Convention on Cybersecurity and Personal Data, and the African Continental Free Trade Area Agreement among others. In Kenya, data localisation requirements are laid down under Section 50 of the Data Protection Act 2019 and Regulation 25 of the Proposed Data Protection (General) Regulations 2021. Kenya's framework is therefore not yet settled as the proposed regulations are currently under consideration after a public participation exercise that ended on 11 May 2021. The aim of this study is to discuss data localisation in the Kenyan context and analyse the impact of these measures on the Kenyan economy. The paper will also review their impact on various regional treaty frameworks, and other agreements. Through analysing Kenya's current data localisation practices, this paper will conclude by providing recommendations on how to successfully implement localisation laws bearing in mind key legal and local economic considerations, as well as regional trade agreements and relations with Kenya's trading partners.

1. INTRODUCTION

Trade as we know it has been revolutionised by improvements in technology. This has increased economic activity across the globe by ensuring connectivity and enhanced communication channels which in turn have led to new businesses, production processes, and new challenges and opportunities. In fact, online access and ease of communication through the free flow of information are the driving force of the digital economy resulting in significant growth of the global economy.[1]

The key driver of this economy is data. Data is referred to as information in electronic form.[2] It is often spoken of as the raw material or the 'oil' of the digital economy. Due to the nature of the internet, the digital economy has been driven by the free flow of data that has made it easy for business to offer their services across the globe. However, recent changes seek to limit this free flow by introducing data flow restrictions on cross-border data flows and transfers. Some of these restrictions include the promulgation of data localisation laws.

Data localisation laws have been defined as 'laws that limit the storage, movement, and/or processing of data to specific geographies and jurisdictions, or that limit the companies that can manage data based upon the company's nation of incorporation or principal situs of operations and management.'[3]

To fully understand the context of data localisation, it is key to note that some of the restrictions imposed are a form of data processing as defined under Section 2 of the Data Protection Act 2019 (DPA). The section defines processing as:

> *...any operation or sets of operations which are performed on personal data or on sets of personal data whether or not by automated means, such as:*
>
> *(a) collection, recording, organisation, structuring;*
> *(b) storage, adaptation or alteration;*
> *(c) retrieval, consultation or use;*
> *(d) disclosure by transmission, dissemination, or otherwise making available; or*
> *(e) alignment or combination, restriction, erasure or destruction.*

Data localisation measures pre-dating the internet era were designed to ensure that governments had access to data when they needed it.[4] Post-internet era, different countries have justified the need to enact data localisation laws using a multitude of reasons including privacy concerns and protection against surveillance by other countries.[5]

Other justifications for adopting data localisation policies include legal issues such as data sovereignty, information sovereignty, data access by governments, extraterritorial application of laws, protection of intellectual property, to help curb computer-related crime and to regulate corporate behavior.[6]

Various scholars argue that these justifications for data localisation do not hold much water, but in turn these laws increase cybersecurity risks and erect barriers to trade and innovation[7] and as such are a mode of digital protectionism and restrictive trade practices.

In Africa, 31 countries out of the 54 have enacted data protection laws as at February 2020. Privacy, as a human right, is primarily enshrined in national constitutions and some countries have gone ahead to enact legislation to realise this fundamental right.[8] Even though some African countries had data privacy and protection laws in place before the GDPR – such as Morocco who requested an adequacy decision in 2009[9] – a majority of countries who have enacted data privacy and protection laws after the GDPR have modelled the laws after the *EU General Data Protection Regulations 2018* (GDPR). In addition, some have been influenced by various regional laws and treaties such as the *Malabo Convention, Smart Africa Initiative, Africa Data Leadership Initiative*,[10] the *African Continental Free Trade Area Agreement* (AfCFTA) and the *Regional Economic Communities Model Laws*.

In Kenya, data localisation requirements were initially codified in sector-specific laws. However, in 2019, the DPA was enacted and it expressly prescribes prohibitions on processing certain types of data outside Kenya. This is prescribed under Section 50, which outlines that:

> *The Cabinet Secretary may prescribe, based on grounds of strategic interests of the state or protection of revenue, certain nature of processing that shall only be effected through a server or a data centre located in Kenya.*[11]

To supplement this provision, the government recently released the *Proposed Data Protection General Regulations*[12] which provide clear directions on what data is restricted to processing in Kenya. These regulations have not yet been formally enacted as at May 2021.

The aim of this study is to discuss data localisation in the Kenyan context and analyse the impact of these measures on the Kenyan economy. The paper will also review their impact on various regional treaty frameworks, and other agreements. The main argument in this paper is that while Kenya is leaning towards strict data localisation measures, the economic impact on Kenya's economy, as well as the implications for Kenya's commitments in regional and international treaty frameworks, require deeper analysis. The recommendations proposed in

this paper include developing a data centre information and communications technology (ICT) infrastructure policy that will set a standard on data governance and promote a responsible data sharing culture, ratifying the African Union Convention on Cybersecurity, and encouraging the use of reciprocal (bilateral) data protection agreements to promote trade and the free flow of information. Other recommendations include promoting African cooperation and joint development of digital regulation frameworks and governance models, and facilitating cross-border data flows in the East African region by signing the East African Community (EAC) protocol and the AfCFTA. In addition, a holistic review of sector-specific laws providing for data localisation requirements is necessary.

From a methodology perspective, this paper has been primarily developed through a qualitative review from data sources such as observations, online commentary and document analysis.

2. DATA LOCALISATION IN KENYA

2.1 Forms of data localisation

The Global Economic Governance Programme (GEG) has categorised data localisation restrictions into five classifications, ranking them from the least to most restrictive measure:[13]

- The first category is the least restrictive measure, which does not impose any restrictions as to data movement and allows the company to decide where to store and process the data.

- The second category allows cross-border data transfers but requires that a copy of the personal data is stored locally. This normally applies to specific types of data such as health data.

- The third category requires that companies store and process data locally using data centres located in the country. This has had a negative impact where companies may choose to leave a jurisdiction if they find it expensive to store and process data locally. Consequences of non-compliance may result in the company's access being blocked. For instance, LinkedIn was blocked from the Russian market for failure to observe Russian data localisation laws.[14]

- The fourth category, bans cross-border sensitive data transfers. This usually applies to sensitive types of data including race, biometric data, religious and political beliefs. In most cases, this data may be transferred with the consent of the data subject and where it can be shown that such transfer is necessary and in the best interest of the data subject. For example, employment record transfers between a parent company and its subsidiary.

- The fifth category requires the fulfillment of certain conditions before any transfer abroad. These conditions may be levied upon the recipient jurisdiction, e.g. countries with adequate levels of protection of personal data or companies showing that data subjects have given their consent to such transfer. For example, this is a requirement in the GDPR where third countries must seek authorisation from the European Commission and be recognised as a country meeting the adequacy standard.[15]

From the categorisation above, the type of data localisation laws in Kenya range from the third to the fifth category. The provisions currently espoused in the proposed general regulations draw on this.

> African countries have also joined this trend and enacted data protection laws with localisation requirements which have rapidly increased since 2013.

Data protection is increasingly an area of importance with countries choosing to protect their data and that of their citizens against exploitation and misuse.[16] Data is now shared, traded and exchanged on a large scale across the globe, whilst being processed and stored in various countries. Most users of the data (and data subjects) are unaware of this situation. This data is stored in the cloud, which refers to servers that are accessible over the internet. These servers are normally stored in various jurisdictions. This trend has grown dramatically due to the ease and efficiency created by cloud computing. Cloud computing has made it easier to access data across the globe and not have to consider the extreme storage costs of owning and operating a data storage facility.

Some African countries have also joined this trend and enacted data protection laws with localisation requirements which have rapidly increased since 2013[17] after the Snowden revelations of surveillance activities by the United States (US) and the United Kingdom (UK), amongst other countries.[18] After these revelations, major economies such as China and Russia sought to change their policies on data localisation and enacted very

stringent data localisation measures including hefty fines and penalties for repeat offenders.[19] Many African countries have enacted data protection laws modelled after the GDPR, which offers a measure of compliance with the adequacy requirement therein so as to attract foreign investments and be in line with international best practice.[20]

2.2 National laws and policies on data localisation in Kenya

2.2.1 Constitution of Kenya 2010

At a national level, laws on privacy and data protection, which include data localisation requirements, get their bearing from the *Constitution of Kenya*. Articles 31(c) and (d) guarantee the right of every person not to have 'information relating to their family or private affairs unnecessarily required or revealed' and the right not to have 'the privacy of their communications infringed'.

It is important to distinguish between data localisation laws and data privacy and protection. As defined above, data localisation laws are laws that require that personal data, depending on the type or nature, be processed in the country of the data subjects. Data privacy is the right of a data subject to control how third parties should use their personal data[21] whereas data protection is the process of safeguarding personal data using technical and organisational measures to protect it against unauthorised access or use.[22]

In addition, Article 21(4) of the constitution mandates the state to enact and implement legislation fulfiling its international obligations with respect to human rights and fundamental freedoms. In line with this, Kenya enacted the DPA in 2019 which is the primary statute with respect to privacy and data protection in Kenya.

2.2.2 Data Protection Act 2019

Data localisation is not defined under the Act, however, Section 50, leaves it to the Cabinet Secretary (CS) to stipulate which personal data should be stored and processed in Kenya on grounds of strategic interests of the state or for the protection of revenue.

Under the Act, data localisation measures are enacted under Section 50. This section stipulates that the CS may prescribe that certain data processing shall only be processed in Kenya. In line with this provision, *general subsidiary regulations*[23] have been drafted in an attempt to create a comprehensive data localisation framework, and to enable compliance with Section 50.

In addition, certain restrictions have been introduced with respect to cross-border data transfers. From the definition above on data localisation measures, any measures that limit or prohibit data transfers are a form of data localisation measures. Under the Act, cross-border data transfers are only allowed if the data controller and data processor meet the conditions specified under Section 48, which states that:

A data controller or data processor may transfer personal data to another country only where —

(a) the data controller or data processor has given proof to the Data Commissioner on the appropriate safeguards with respect to the security and protection of the personal data;

(b) the data controller or data processor has given proof to the Data Commissioner of the appropriate safeguards with respect to the security and protection of personal data, and the appropriate safeguards including jurisdictions with commensurate data protection laws;

(c) the transfer is necessary —

i. for the performance of a contract between the data subject and the data controller or data processor or implementation of pre-contractual measures taken at the data subject's request;
ii. for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another person;
iii. for any matter of public interest;
iv. for the establishment, exercise or defence of a legal claim;
v. in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or
vi. for the purpose of compelling legitimate interests pursued by the data controller or data processor which are not overridden by the interests, rights and freedoms of the data subjects.

The Act prohibits cross-border data transfers unless such transfers are to a country with adequate levels of protection, the same as in Kenya, or approvals have been obtained after the data controller or data processor has given sufficient proof that measures have been put in place to protect the personal data.

Further, Section 49, with respect to sensitive data states that:

> *Sensitive data may only be transferred outside the country where the data subject has given express consent, effective and appropriate safe-guards have been put in place and in line with*

the requirements or conditions set by the Data Commissioner.

To operationalise the effect of Section 50 of the Act, Regulation 25 of the *Proposed Data Protection General Regulations 2021* stipulates that:

> *…a data controller or data processor who processes personal data for the purpose of actualizing a public good, set out below, shall be required to ensure that such processing is affected through a server and data center located in Kenya, and at least one serving copy of the concerned personal data is stored in a data center located in Kenya.*

The 'public good' contemplated under this Regulation includes:

(a) Administering a national civil registration system including registrations of births and deaths, persons, adoption and marriages;

(b) Operating a population register and identity management system including any issuance of any public document of identity;

(c) Managing personal data to facilitate access to primary and secondary education in the country;

(d) The conduct of elections in the country;

(e) Managing any electronic payments systems licensed under the National Payment Systems Act;

(f) Any revenue administration system for public finances;

(g) Processing health data for any purpose other than providing health care directly to a data subject; and

(h) Managing any system designated as a protected computer system in terms of section 20 of the *Computer Misuse and Cybercrime Act 2018.*

Interesting to note is the choice of words in the two pieces of legislation. Section 50 of the DPA states that the measures put in place should be with respect to the 'strategic interests of the state or for the protection of revenue'. Regulation 25 on the other hand, states that these measures are 'for the public good.' Both terms are not defined under the Act or regulations. This inconsistency may open room allowing additional data localisation measures to be put in place on grounds of the overtly broad 'strategic interest of the state'. For example, research conducted by the Kenya ICT Action Network (KICTANET) shows that in April 2019, the government of Kenya deployed the integrated Public Safety Communication and Surveillance System that includes facial recognition to help security forces curb crime. As much as this system was deemed to be useful during the break of the COVID-19 pandemic to help in ensuring government guidelines were followed, the surveillance and monitoring system infringes on people's rights to freedom of expression and privacy.[24]

Prior to the enactment of the DPA, data protection and localisation laws were already in existence. These laws are broadly in line with the provisions prescribed in Regulation 25 with respect to various sectors termed as personal data relating to personal good. If the regulations pass as they are, then data localisation requirements shall manifest primarily under the DPA and secondarily, under industry-specific laws as described below.

> Data privacy is the right of a data subject to control how third parties should use their personal data.

2.2.3 Information technology and telecommunications sector regulations

The Kenyan ICT Framework Policy[25] requires that Kenyan government data remains in Kenya and is stored in a manner that ensures privacy for its citizens. In addition, the national government has encouraged the county governments to create shared data centres where all government data will be stored. The Ministry of ICT has refused to approve new investments where there is available capacity to store and process data in the country.

Section 27(2) of the *Kenya Information and Communications Act (KICA)* mandates the Minister (CS), in consultation with the Communications Authority of Kenya (CAK), to make regulations with respect to the privacy of telecommunication data.

The Kenya Information and Communications (Registration of Sim-Cards) Regulations 2015 require that telecommunications operators grant CAK officers access to its systems, premises, facilities, files, records and other data to enable the authority to inspect the data to ensure compliance with the Act. To ensure access and availability for inspection by CAK, this has been interpreted in practice that such data should be stored in the country. For example, Safaricom (the largest mobile network operator in Kenya) has two data centres in two Kenyan towns, Thika and Kisumu, where they store personal data such as communication data and subscriber data.

The Kenya Information and Communications (Consumer Protection) Regulations 2010 lays down privacy and data protection requirements in telecommunications by service providers[26] and a service provider is under a duty to provide all communication data, which includes personal data in the event of an emergency.[27] Arguably, from the author's experience in legal practice when dealing with National Security agencies, such data may be required to be stored in the country so as to enable quick and easy transfer to the respective emergency service providers in the event of an emergency.

Section 50 of the *Computer Misuse and Cybercrimes Act 2018* stipulates that, where a police officer or an authorised person has reasonable grounds to believe that specified data is stored in a computer system in possession of a person in Kenya, or the subscriber information relating to services rendered by a service provider in Kenya is in the control of that service provider, that officer may apply to a court for a production order for that information.

2.2.4 Health sector regulations

Health data is a type of sensitive personal data as described under Section 2 of the DPA. It states that:

> *'Sensitive personal data' means data revealing the natural person's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of the person's children, parents, spouse or spouses, sex or the sexual orientation of the data subject.*

In addition, the same section defines health data as:

> *data related to the state of physical or mental health of the data subject and includes records regarding the past, present or future state of the health, data collected in the course of registration for, or provision of health services, or data which associates the data subject to the provision of specific health services.*

The *Health Act 2017* has data privacy and protection provisions. Section 11 provides that information concerning a user related to their health, status, and treatment is confidential unless such disclosure is required through a court order or where a user gives informed consent for the use of their health data for health research and policy planning purposes. When read together with Section 49 of the DPA, this provision amounts to data localisation measures that restrict the processing of health data.

In addition, the *HIV and AIDS Prevention and Control Act 2006*, under Section 20 stipulates that storage, transmission and collection of data of persons tested must be in line with guidelines on confidentiality prescribed by the minister in charge of health. No such guidelines have been put in place, thus the primary statute regulating such disclosure and any further processing is the DPA. In this regard, health data forms part of sensitive data, of which its processing is limited under Section 49.

2.2.5 Security sector regulations

Under Section 45 of the *Private Security Regulation Act*,[28] a Private Security Service Provider[29] is under an obligation to share all information it obtains in the course of duty with the National Police Service for the purposes of preventing crime, apprehending a person, sharing actionable intelligence or any information that is necessary for any other lawful purpose.

Such information is required to be accessible on demand at least six months after obtaining the information.[30] This requirement may be interpreted to mean that the information must be readily available and accessible. The act does not prescribe explicit localisation measures but the wording of this section, 'on demand' may dictate that such data should be within the control and reach of the provider without any immediate limitations on accessing the data.

> Privacy and data protection laws in Kenya are greatly influenced by international laws and best practices.

2.2.6 Elections regulations

Before elections are conducted, voter registration must be carried out using election technology selected by the Independent *Electoral and Boundaries Commission (IEBC)*. In line with this, the IEBC enacted the Election (Technology) Regulations 2017. The regulations provide that the commission shall put in place measures to ensure data availability, accuracy, integrity and confidentiality. The first schedule lists such measures to include a data centre facility where access to the data centre is limited to authorised personnel, database management systems and ICT governance.

In addition, the commission is required to store and classify data[31] in accordance with the principles and provisions of the *Access to Information Act*.[32] Also, Regulation 17 stipulates that all electronic data relating to an election shall be stored by the commission for a period of three years after the election results have been declared. The commission shall also maintain an external

data recovery site for all electoral information systems.[33] This data includes personal data of those who turn out to vote during elections. This is also in line with the provisions of Regulation 25 of the *Proposed Data Protection (General) Regulations 2021*, which highlight election data as data that should be stored and processed in the country for the public good. Elections have been a very volatile subject and exercise in the past, which has led to post-election violence due to 'perceived' impropriety in vote counts and tampering with election data. Thus, it is the authors' view that this requirement in itself does not necessarily mean that it is for the public good or addresses the perception challenge by ensuring authentication of the results. As observed in the 2017 general elections, computer servers at the national tally centre failed. This technical failure was one of the grounds cited by the Supreme Court of Kenya for the nullification of the general elections. Thus, localisation measures do mean efficiency or transparency in this instance.[34]

2.2.7 Government ICT systems and repositories regulations

The government has ICT-based surveillance systems that collect substantial amounts of personal data. These systems include: the Network Early Warning System (NEWS), the National Surveillance Communication Command and Control Systems (NSCCCS) which is based on CCTV surveillance on the streets, the Device Monitoring System (DMS) and the Biometric Immigration Services.[35] It is not clear where this data is stored, however, Section 36 of the *National Intelligence Service Act 2012* states that the right to privacy of a person which is enshrined in the Constitution of Kenya Article 31 may be limited where a person conducts an offence.

Thus, Section 45 of the same Act empowers an officer to obtain any information, material, record, obtain access, to search and remove or examine any information, material or document as well as to monitor communication or install, maintain or remove anything associated with the investigation at hand.

Regulation 25(h) of the general proposed regulation read together with Section 5(i) of the *National Intelligence Service (NIS) Act*[36] requires the NIS to safeguard information systems and processes within state agencies. This may require that, for example, telecommunications data and CCTV be stored locally to enable easy monitoring and investigation as well as to enable the production of such information as evidence in a court of law, which is in line with their mandate of ensuring national security.

Also, the government has an Integrated Population Registration System (IPRS) which is a collection of registries – marriages, birth and deaths, ID register, aliens and refugees register, passport register, tax, insurance, national transport systems authority register, banking institutions, credit reference bureau, among others. This data is required to be stored in Kenya under the control of the Ministry of State for Immigration and Registration of Persons.[37] This is also the position as stated under Regulation 25 of the *Proposed Data Protection (General) Regulations*.

2.3 International factors affecting Kenya's privacy and data localisation laws

Privacy and data protection laws in Kenya are greatly influenced by international laws and best practices. The tension here for Kenya being the need to develop a legislative framework that facilitates data protection as well as economic growth, innovation and trade between Kenya and its desired trading partners. This factor underpinned the DPA being greatly influenced by the GDPR 2016 and more specifically the *UK Data Protection Act 2018*.

In addition to the above, some of the international instruments influencing data privacy and protection in Kenya include:

- The *International Covenant on Civil and Political Rights* (ICCPR) under Article 17 recognises the right to privacy. Kenya has ratified this convention.

- The *Universal Declaration on Human Rights*[38] under Article 12, which stipulates that no one shall be subject to arbitrary interference with his family, home or correspondence and that everyone has a right to protection against such interference.

Kenya and the US are currently in negotiations for a proposed *US-Kenya Free Trade Agreement*. If agreed upon, this would be the first trade agreement of its kind in Kenya and East Africa, and it may provide a framework and template for strengthening US relationships with economies across the continent. This is in line with the provisions of the *African Growth and Opportunity Act* (AGOA) which comes to an end in 2025.[39]

During the current negotiation period, the US envoy, who opposed the imposition of unilateral regulations and taxes as the US finds these laws discriminatory against US organisations in Kenya, raised concerns.[40] These concerns were raised in respect of the data localisation requirements under the DPA and the introduction of the *Digital Services Tax* (operational from January 2021) which imposes a tax on income derived or accrued in Kenya from services offered through a digital marketplace. The US's objective in taking this stance is to remove (in their view) discriminatory and restrictive measures against their institutions that would negatively impact digital trade.

As the negotiations are still ongoing, it remains to be seen whether these negotiations will lead to recommendations that impact Kenya's data protection laws that are new and still being developed. There may be future opportunities to negotiate amendments to incorporate and balance the interests of both parties.

2.4 Regional laws and treaty frameworks on privacy, data protection and trade

At a regional level, the *African Charter on Human and People's Rights 1981*[41] does not have any provision on privacy and data protection. However, the *Malabo Convention 2014*[42] sets out substantive provisions on data protection that all member states who have ratified the convention must comply with.

With respect to data localisation, the Convention prohibits cross-border data transfers unless there is an adequate level of protection.[43] The challenge with this provision is that the term 'adequate' has not been defined under the convention. Thus it has been left to member states to define what adequate measures means in their respective context. To expound on this further, various countries have various standards and requirements with respect to cross-border data transfers. Thus, any organisation seeking to transfer data abroad should first ensure that they have in place measures like those required from the exporting country. On the other hand, data protection authorities/regulators in various jurisdictions have been given the power to authorise cross-border data transfers. This means the data protection authorities have the leeway to decide and authorise what data may be processed and transferred outside a country and which data cannot.[44] This presents a challenge for organisations that have branches and subsidiaries across Africa. Thus, different legal systems mean different forms and levels of compliance that may be costly for organisations to comply with and lead to conflict of laws.

The *African Union Convention on Cybersecurity and Personal Data Protection*, also known as the Malabo Convention was enacted with the intent of ensuring data privacy and protection across the continent. The aim of the convention is:

> *...to set up a minimum standards and procedures to reach a common approach on the security issues in Africa and address the need for harmonized legislations necessary to enhance cooperation in the area of cybersecurity in Member States of the African Union.*[45]

However, there have been challenges in the ratification of the convention by member states. For instance, as at February 2020, only five countries have ratified the convention and another 13 have only signed but not ratified the convention since it came into force in 2014. Kenya has not signed the convention. The challenges that have made this difficult include significant cultural differences, different privacy expectations, regulatory frameworks, technology capacity as well as high dependency on non-African manufacturers and service providers across the continent. These challenges have frustrated attempts to implement the convention uniformly.[46]

To cure this, the African Union (AU) in collaboration with the Internet Society developed the *Privacy and Personal Data Protection Guidelines for Africa*[47] that set out recommendations and a blueprint for state actors who are in the process of developing policy on privacy and data protection.

The challenges that have made this difficult include significant cultural differences, different privacy expectations, regulatory frameworks, technology capacity as well as high dependency on non-African manufacturers and service providers across the continent.

The *East African Framework for Cyberlaws 2010* vision is to increase production, trade and investments in the East African region through ICT. To ensure this, the framework is meant to harmonise laws affecting the use and implementation of ICT. On privacy and data protection, the framework lays down the key principles of data processing including fairness, accountability and transparency, among others. However, key concerns have been raised with respect to the 'cost of regulation'.[48] For Kenya, with respect to data localisation, a data controller and data processor must notify the commissioner under Section 48 of the DPA, when transferring data outside Kenya. The proposed regulations[49] do not require the data controller and data processor to pay any fees to the commissioner but require that the parties enter into agreements, which may be costly due to different legislative frameworks.

Kenya is a member of the EAC. One of its key pillars to enable trade in the community is to allow the free movement of services including the free flow of education, science and technology.[50] To this end, the EAC enacted *The East African Community Common Market Protocol 2009*,[51] and Kenya is a signatory. The Protocol provides for the free movement of goods, persons, labor, services, capital and establishment.[52] This is premised on

the objective of accelerating economic growth and development of partner states by ensuring free flow of people, goods and services. To this end, the member states agreed to eliminate tariff, non-tariff and technical barriers to trade by implementing a common trade policy for the community.

Furthermore, to ensure economic growth and cooperation, member states[53] agreed to ease cross-border movement by removing restrictions on the movement of persons and services. The community has agreed to establish a standard identification system of issuing national identification documents that will be the basis for identifying citizens of partner states within the community.[54] In addition, such identification cards will be[55] electronic which will enable free movement of people in the community.

With respect to data localisation, the protocol has not made it clear how this will be implemented and where the personal data collected, under the standard identification system, will be stored. This has led to the slow implementation of this system.[56]

Currently, personal data of data subjects of the EAC is stored at a national level, for example, government data with respect to immigration. The existing framework protocol, therefore, does not provide substantive provisions on data compilation for the common market. However, if this recommendation is implemented, Kenya may have to revise its laws to align with the intention of the Common Market Protocol and the new framework. Regulatory divergence may create a problem for investors looking to invest within the EAC thus hindering development and economic growth.[57]

AfCFTA is the AU's flagship project of the AU Agenda 2063, which is Africa's blueprint for transforming Africa into a powerhouse and for attaining inclusive and sustainable development in the continent. This will be the largest free trade area bringing together all the 55 member states with a population of approximately 1.2 billion and a combined GDP of approximately USD3.4 trillion.[58]

Currently, 36 countries have ratified the agreement and Kenya is among them. Some of the key provisions with respect to data localisation include a commitment to liberalise trade in services,[59] governed by principles on transparency and information disclosure. This has settled any issues arising from inconsistencies between the agreement[60] and regional agreements by establishing that the AfCFTA takes precedence.[61]

The *AfCFTA Protocol on Trade in Services* defines trade in services to include the supply of a service from the territory of one state party into the territory of another state party.[62]

With respect to cross-border data transfers, the protocol does not explicitly prohibit such transfers but provides that member states have a right to regulate matters enshrined in the agreement.[63] In addition, Article 13 on payment and transfers provides that parties are prohibited from applying restrictions on international transfers and arguably international money transfers.

With respect to trade in services, every member state has general obligations under Part IV to trade fairly with other member states and remove any restrictions that would inhibit trade in services. Data localisation requirements have been regarded as measures that inhibit trade and thus termed to be restrictive and against the World Trade Organisation (WTO) laws on enabling trade without any restriction.[64]

However, Article 15 provides general exceptions where restrictions may be allowed. These include measures to protect public interest and morals, measures necessary to protect humans, animals or plant life, and measures necessary to protect the privacy of individuals in the processing and dissemination of personal data among others. Thus, Sections 48-50 of Kenya's DPA may fall under these exceptions because the localisation requirements are pegged on public interest.

3. KEY DRIVERS AND EFFECT OF DATA LOCALISATION LAWS IN KENYA

The key drivers of data localisation measures in Kenya are based on the enacted DPA and the proposed regulations. They include:

3.1 Protection and collection of revenue

Kenya has been facing economic challenges particularly given the COVID-19 pandemic. This has led to increased measures to raise revenue through taxation of citizenry and local and international businesses. This has necessitated the government's taxation policy makers to effect measures to track and access financial data.

An example of a recent taxation development is the *Digital Services Tax* introduced in 2020. This tax is payable by a digital service provider or digital market provider or their representative. For a non-resident, they shall be liable by virtue of providing services in Kenya from a terminal in Kenya, where the payment of the service is made using a debit or credit card of a financial institution in Kenya. The service is acquired through an internet protocol address registered in Kenya or if the business has a billing address in Kenya.

For the Kenya Revenue Authority (KRA), Kenya's taxation agency, to determine these key details, they must have access to the above data. Through mandating that this data be held in Kenya and accessible to KRA, the taxation agency can increase their visibility of these non-resident entities and collect revenue for the Government that they would otherwise have been unable to. This of course is seen as positive for revenue collection.

3.1.1 National security

Like many countries, data localisation laws in Kenya are driven by government concern for protection against acts of terrorism, sabotage and technical faults, protection of critical infrastructure and other national security concerns. In line with this, the government created a tier-2 Government Data Centre (GDC) in 2008, to host crucial government data[65] and a Critical Infrastructure Protection Unit (CIPU).

However, whilst storing data on local servers may increase the effectiveness of law enforcement, grant governments more jurisdictional control over data, and amplify governments' surveillance potential, it will do very little to safeguard the privacy and security of users despite such claims by governments.[66]

While it may make sense to provide guidelines for dealing with data deemed sensitive to national security, care must be taken to ensure that it does not impede corporate innovation.[67] Lack of privacy and security of data subject's data is a key factor in impeding investment and innovation.

Storing all the consumer data inside a geographical region may also heighten negative externalities by risking that data might be broken into, at the orders of a government, or because of a lack of adequate security systems.[68]

3.2 Cloud computing

Cloud computing services offer flexible and affordable software, platforms, infrastructure and storage available to different organisations across numerous industries. This presents an opportunity for organisations to reduce the cost of conducting business, increasing flexibility and improving IT capabilities such as interoperability.[69]

This is particularly important for the Kenyan economy considering that the largest segment of the population is made up of the youth, who are the drivers of the gig economy, entrepreneurs and innovators. As a comparative example, research shows that a company would pay 54% less using cloud services hosted outside Brazil vis-à-vis utilising hosting services within Brazil.[70] In Kenya, Google offers its customers free cloud storage of 15 GB but on exhausting that, it gives them a choice to pay Sh200 for 100 GB or Sh300 for 300 GB per month. For heavy file storage, you are required to part with Sh1,000 for 2 TB of storage, Sh10,000 for 10 TB, Sh21,000 for 20 TB or Sh31,000 for 30 TB, according to your demand, per month.

A local host, like Safaricom, on its part, offers the same services at an extremely high price of 100 GB at Sh1,392, 400 GB at Sh4,872, 1 TB at Sh12,110, 5 TB at Sh59,624 per month while those who opt for 20 TB of storage will have to pay Sh237,800 per month.[71]

This difference in cost provides a huge competitive edge for any business, and particularly for younger entrepreneurs who in many instances face capital expenditure challenges when starting up and running their businesses.

Kenya's economic growth relies on the great promise of innovation and ICT. To encourage this growth, measures that encourage investment, and reduce barriers of entry to business have to be put in place. Stifling the use of cloud computing through overly restrictive data localisation laws (e.g requiring only the use of more expensive local alternatives and data centres) impedes investment and increases barriers of entry to business thus impacting the development of our economy.

3.3 Economic output

The value of data is created when the data is used, analysed, manipulated and transmitted to create an output through innovation or the creation of new services that increase efficiency and add value to society.

Since data localisation may restrict the ability of businesses and individuals from making full use of data, and in effect increase the cost of services that require data, it stands to reason that prices of any goods or services that use data in their production would also increase. In many sectors of the economy, data localisation may lead to productivity losses at a domestic level.

Data localisation laws may have a direct impact on various sectors of the Kenyan economy as they may reduce connections to digital trade, stifle innovation, restrict access to new and advanced technology, block competition and add to the cost of maintaining local data infrastructure.

The US has minimal data localisation requirements even though recently there have been talks of introducing strict localisation measures mostly targeting China.[72] The absence of these laws has enabled the evolution of the internet and creation of big tech giants who have revolutionised how we use the internet today. For example, in 2019, the global retail e-commerce sales

reached USD3.53 trillion thus promoting the economic output and opening up the country to the world.[73] This illustrates the great potential of harnessing the power of data without any restrictions that inhibit innovation.

Conversely, there is the argument in many quarters by policy makers that these restrictions boost the economic activities within the country and as a result promote economic growth and output. For instance, it has been argued that the requirement for data localisation laws for national security, privacy, consumer preferences and liability concerns for businesses will create market demand for regional and local data centres, and for software and hardware that facilitate geographical localisation.

Kenya's proposed laws are quite restrictive on what data may be stored outside the country.

Such restrictions will only benefit Kenya in the short term. In the interim, these laws may create jobs and attract foreign direct investment on ICT with respect to infrastructure and resources required. However, in the long term, these restrictions will raise the cost of conducting business because organisations will only be limited to resources within the country. For example, Kenya has approximately ten data centres.[74] Strict implementation of these restrictions means that the supply and demand ratio will increase and cost organisations a lot of money to ensure compliance with data localisation laws.

Beyond this, it affects Kenya's participation in regional trade through various treaty frameworks. Kenya's proposed laws are quite restrictive on what data may be stored outside the country, and this challenges some of the gains that the AfCFTA and the *EAC Common Market Protocol*, for example, seek to achieve.

3.4 Data centres

Kenya currently has approximately ten data centres serving a population of approximately 50 million. Given the data localisation requirements, more data centres will have to be created.[75] The hardware required to operate data centres is expensive thus increasing the required initial investment.

Challenges in developing and maintaining data centres in Kenya include:[76]

(a) Lack of smart data centres to host local and international internet exchange and content delivery networks;

(b) Lack of functional recovery data centres – Kenya's mode of operation is using a centralised mode of data governance thus putting key data at risk of breach or destruction;

(c) Lack of adequate power supply and no power backup;

(d) Lack of integrated monitoring for data centres;

(e) Lack of proper capacity, i.e. infrastructure to host all government institutions and personnel; and

(f) Lack of a sustainability model for government cloud and data centres.

Lack of resources and adequate skills to maintain these data centres also presents a huge problem. The cost of maintaining these data centres is exacerbated by massive electricity requirements and reliance on skilled labor that is currently unavailable in Kenya. Thus, it is inevitable that the above costs would be transferred to consumers who are already burdened with the current high cost of living.

Further, data centres are highly automated, hence, there may be job offerings at inception but once the data centre is complete most of those employed will be made redundant. Thus, a rise in the creation of data centres will not automatically translate into the creation of jobs in the long term.

3.5 Internet of things (IoT)

The Internet of things (IoT) is exponentially growing, driven by cloud computing and advanced data analytics. Kenya has ample data to ensure the steady growth of IoT from cell phone data, social media, CCTV, traffic cameras, global positioning systems and banks. The government has recognised the importance of IoT and to this end, the Communications Authority of Kenya issued guidelines on the use of IoT devices in Kenya.[77]

Advantages of IoT include increased productivity, enhanced energy of cost efficiencies and low environmental impact. Key industries affected by IoT include agriculture, manufacturing, transport, logistics, healthcare and education. Data localisation laws affect IoT in that these restrictions increase the costs of implementation as well as lead to duplicity of data.

In 2019, Kenya's largest mobile network operator Safaricom and the Kenya Breweries Limited (KBL) partnered to

enhance KBL cooler systems using IoT technology. This has helped to generate business insights that will assist KBL to optimise their coolers.[78] Also, in 2019, Safaricom partnered with Upepo Technologies, an IoT service provider in Kenya, to enable remote monitoring of water supplies for the Embu Water and Sanitation Company to help match supply and demand. The implementation of overly restrictive data localisation measures will inhibit such innovative solutions that seek to enhance efficiency in provision of key services.

3.6 Barriers to trade

Research shows that data localisation laws may act as a barrier to digital trade where the legislation passed, even though legitimate, may be discriminatory to trading partners. For example, restrictions on financial data, telecommunications and health go against the interest and intention of the AfCFTA, which seeks to open up the African content to trade between countries without strict restrictions as elaborated previously. Thus, the WTO does not allow such legislation with respect to trade in goods as laid down in the *General Agreement on Tariffs and Trade* (GATT).[79] These same principles were incorporated in the *General Agreement on Trade in Services* (GATS), which is aimed at achieving progressive liberalisation of trade in services. This is relevant as Kenya is a member of the WTO and thus bound by the provisions in GATS. The same principles under GATS have been adopted under the AfCFTA protocol on Trade in Services.

The four modes of supply of services under GATS include the cross-border supply of services, consumption of services abroad, commercial presence abroad, and provision of services to consumers in another member state.[80]

Member states are required to immediately and unconditionally accord each member state treatment that is not less than that accorded to like services and suppliers of other member states.[81] This primary objective gives weight to other general objectives under GATS as it is regarded as a minimum standard of treatment of services and suppliers in all sectors of the economy.

This is the same position as under the AfCFTA *Protocol on Trade in Services*, Article 4 and under the EAC *Common Market Protocol*, which Kenya is a signatory to. Article 4(3) stipulates that to realise and attain the objectives of the protocol, member states shall harmonise and integrate their policies in the areas provided under the protocol. To ensure this, Article 5 stipulates the scope of cooperation in the common market, which includes removing restrictions on the movement of people, goods and services.

Kenya's laws on cross-border data transfers require that the country where the data is sent to must meet certain conditions such as ensuring safeguards and adequate levels of protection in the other country.[82] The EAC protocol may be a means of ensuring adequacy status within the community but such transfers are still problematic to countries outside the community who do not have similar or adequate measures of protection of personal data.

Human rights extend to the digital space and hence require protection.

To try and resolve this, the *Proposed General Regulations* in Kenya stipulate that another level of adequacy would be to permit transfer with countries that are signatory to the *African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention)*. However, despite this proposal, Kenya is not a signatory to this convention. Reciprocal requirements are the norm in many of these treaties, therefore, Kenya's advocacy for the *Malabo Convention* as an adequacy status requirement in the proposed regulations without being a signatory must be addressed by our policy makers.

Kenya must consider these international and regional treaty frameworks as it settles its data localisation laws or risk the loss of opportunities that trading with these partners affords.

3.7 Impact on human rights and freedoms

A country's human rights record poses a credible economic development and reputational risk and impacts its economic status, as trade bans and restrictions are tools used to influence human rights across the globe. Human rights extend to the digital space and hence require protection. The rights to online privacy and freedom of expression, for example, are extensions of the equal and inalienable rights laid out in the *United Nation's Universal Declaration of Human Rights*.[83]

Data localisation laws may expose Kenyan citizens to government surveillance, breaches of privacy and cybercrime. On the one hand, access to this data allows law enforcement to investigate and prosecute crime without hindrance, and intelligence services can detect any activity that is contrary to the national security interests. However, this access may easily be misused by government agencies through surveillance of the citizenry without their knowledge or consent.

This may interfere with human rights and freedoms enshrined under the *Constitution of Kenya 2010* and beyond this. It may also breach the provisions of the *Universal Declaration on Human Rights 1948 Articles 12 and 19* of which Kenya is a signatory.

4. RECOMMENDATIONS

Whilst Kenya's laws on data localisation are not yet settled, a review of the current proposed regulations indicates that Kenya is leaning towards strict data localisation measures. The government should have a comprehensive and strategic data localisation position that considers the impact on Kenya's economy as well as regional and international treaty frameworks including:

- Developing a data centre ICT infrastructure policy that will set a standard on data governance and promote a responsible data sharing culture both within the country and externally to ensure innovation whilst reducing the cost of hosting data.

- Considering the impact of strict data localisation measures on digital rights as a legislative framework that impinges on these may prove a deterrent for regional and international trade and may cause harm to individuals and society.

- Signing and ratifying the *Malabo Convention* before requiring other countries to do so as a means of meeting the adequacy requirement. This action will signify Kenya's commitment to intra-African partnership and will enhance cooperation in the continent.

- Encouraging the use of reciprocal (bilateral) data protection agreements, Kenya should consider developing these with specific countries to promote trade as it settles its broader international and regional treaty framework position. These agreements are now becoming common and beneficial to the respective countries. For example, the *Australian-Singapore Digital Economy Agreement*, entered in 2020, enables free flow of information in the two countries.

- Promoting (across Africa) cooperation and joint development of digital regulation frameworks and governance models encompassing data localisation provisions that are nuanced towards Africa's specific requirements.

- Facilitating cross-border data flows in the East African region by signing the EAC *Common Market Protocol* and the AfCFTA. To meet its obligations, it should remove unnecessarily restrictive data localisation measures to fully realise and benefit from the free flow of data that these frameworks will afford.

- Undertaking a holistic review of sector-specific laws providing for data localisation requirements. The enactment of the DPA 2019 has led to the realisation of a standard legislative framework on privacy and data protection. The existence of sector-specific restrictions may lead to duplicity, failure of compliance due to different standards, as well as establishing a different threshold for protection apart from the one established under the DPA.

- Seeking out other forms of addressing key issues that have encouraged localisation laws. For example, just like the US, consider how policy may help in addressing law enforcement and national security concerns pragmatically:

    - » As governments no longer have the ability to independently and easily enforce laws, manipulate data and information flow, and secure privacy and security without relying on intermediary companies' infrastructure (e.g. Google, Facebook, etc), governments can increasingly access user data by imposing law enforcement requests on information intermediaries such as search engines, social media, and e-mail platforms.[84]

    - » It is therefore important for the Kenyan government to build relationships with these organisations and use these companies' resources for their self-interest rather than unilaterally developing data localisation measures.

    - » When looking holistically at data privacy laws, policy makers should (influence) encourage the implementation of privacy standards into these private companies' technical and policy infrastructure.

5. CONCLUSION

Data localisation laws enacted in Kenya (as currently drafted) seek to provide privacy and protection for data subjects as well as ensure national security. These laws are not yet settled, with subsidiary legislation currently being considered by policy makers. This offers Kenya a unique opportunity to walk the tight rope between considering its national security objectives and the impact restrictive data localisation measures will have on its economy, trade objectives and human rights record.

The digital economy is driven by the transfer, access and storage of data. The introduction of any restrictive data localisation measures may impede the ability of businesses and individuals from making full use of data, and in effect, increase the cost of services that require data. It therefore follows that prices of any goods or services that use data in their production would also increase thus having a negative impact on Kenya's economy. Any great strides Kenya has made in ICT will therefore stagnate and businesses looking to invest in Kenya will opt to venture out to other countries that have more favorable laws.

The ambit of national security and protecting the digital privacy and cybersecurity of the citizenry falls within government and they rightfully should consider measures to implement this responsibility. This is necessary as businesses enact their policies to maximise revenue by enabling data collection and analytics, and do not always prioritise users' privacy and security.[85]

As the environment in the US has shown, minimal legal intervention on data transfers across jurisdictions has helped create universal and interoperable networks of communication. These networks, in turn, promote access to knowledge and empower individuals to advocate for their rights. They also increase economic activity across jurisdictions by providing services to various industries, enabling digital trade, raising competition, and reducing costs.[86]

Hence, there is a need to reevaluate the options for balancing companies' needs and governments' legitimate need to access data for national security. The answer perhaps lies in the Kenyan government working with its citizens, organisations and trading partners to enact sensible data localisation regulatory frameworks. A key factor to enable this will be government building relationships with private organisations to influence their policies and practices and encourage implementation of privacy standards that will still allow these companies to thrive and innovate.

From a regional treaty framework, as was undertaken in the EU during the development of the GDPR, Kenya and its African trading partners must promote cooperation and joint development of digital regulation frameworks and governance models encompassing data localisation provisions that are nuanced towards Africa's specific requirements. Without this, the current fragmented approach in Africa will continue with the development of frameworks that have been drafted but remain unratified or not implemented. Challenges such as significant cultural differences, different privacy expectations, regulatory frameworks, technology capacity as well as high dependency on non-African manufacturers and service providers across the continent, will continue to frustrate attempts to implement these frameworks uniformly.

ABBREVIATIONS AND ACRONYMS

AfCFTA	African Continental Free Trade Area Agreement
AGOA	African Growth and Opportunity Act
AU	African Union
CAK	Communications Authority of Kenya
CIPU	Critical Infrastructure Protection Unit
CS	Cabinet Secretary
DMS	Device Monitoring System
DPA	Data Protection Act
EAC	East African Community
GATS	General Agreement on Trade in Services
GATT	General Agreement on Tariffs and Trade
GDC	Government Data Centre
GDPR	General Data Protection Regulation
GEG	Global Economic Governance
ICCPR	International Covenant on Civil and Political Rights
ICT	Information and Communications Technology
IEBC	Independent Electoral and Boundaries Commission
IoT	Internet of Things
IPRS	Integrated Population Registration System
KBL	Kenya Breweries Limited
KICA	Kenya Information and Communications Act
KICTANET	Kenya ICT Action Network
KRA	Kenya Revenue Authority
NEWS	Network Early Warning System
NIS	National Intelligence Service
NSCCCS	National Surveillance Communication Command and Control Systems
UK	United Kingdom
US	United States
WTO	World Trade Organisation

ENDNOTES

1 Martina Ferracane. *South Africa and data flows: How to fully exploit the potential of the digital economy*, 2018.
2 M. Irfan. *Data Flows, Data Localisation, Source Code: Issues, Regulations and Trade Agreements*. Geneva: CUTS International, Geneva, 2019. p. 8.
3 Jonah Force Hill. *The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders*, 2014.
4 Supra note 1.
5 https://www.tandfonline.com/doi/full/10.1080/23738871.2017.1402942 Accessed 27 August 2020.
6 William J. Drake. *Background Paper for the workshop on Data Localization and Barriers to Transborder Data Flows 2016*.
7 Supra note 3.
8 Ibid.
9 https://iapp.org/news/a/where-does-africa-stand-ahead-of-the-gdpr/ Accessed 1 July 2021.
10 https://www.uneca.org/storys/eca-smart-africa-future-state-launch-africa-data-leadership-initiative.
11 *Data Protection Act*, 2019.
12 https://www.odpc.go.ke/wp-content/uploads/2021/04/Data-Protection-General-regulations.pdf .
13 Supra note 1.
14 https://iapp.org/news/a/why-linkedin-was-banned-in-russia/ Accessed 27 August 2020.
15 Article 45.
16 Torbjörn Fredriksson, Cécile Barayre and Olivier Sinoncelli and Chris Connolly. *Data Protection Regulations and International Data Flows: Implications for Trade and Development*, 2016.
17 Graham Greenleaf and Bertil Cottier. *Comparing African data privacy laws: International, African and regional commitments*, 2020.
18 https://www.engage.hoganlovells.com/knowledgeservices/news/new-bill-imposing-increased-fines-for-violations-of-russian-data-protection-laws-under-consideration.
19 https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en.
20 Alex B. Makulilo. *"One size fits all": Does Europe impose its data protection regime on Africa?* 2013, p.7.
21 https://www.emotiv.com/glossary/data-privacy/.
22 https://searchdatabackup.techtarget.com/definition/data-protection.
23 https://www.odpc.go.ke/wp-content/uploads/2021/04/Data-Protection-General-regulations.pdf .
24 Sigi Waiguma Mwanzia, Victor Kapiyo and Phillip Ayazika. *Surveillance, data protection, and freedom of expression in Kenya and Uganda during COVID-19 April 2021*. p.15.
25 https://www.ict.go.ke/wp-content/uploads/2019/12/NATIONAL-ICT-POLICY-2019.pdf. p.9.
26 Regulation 15.
27 Regulation 19.
28 No.13 of 2016.
29 Regulation 26 – *The Private Security (General) Regulations 2019*.
30 Regulation 26(2)(b).
31 Regulation 15.
32 No.31 of 2016.
33 Regulation 25.
34 https://www.aljazeera.com/opinions/2013/3/29/technology-transparency-and-the-kenyan-general-election-of-2013.
35 https://www.apc.org/sites/default/files/Data_protection_in_Kenya_1.pdf .
36 2012.
37 https://www.icao.int/Meetings/mrtd-symposium-2014/Documents/7_am_Edaps.pdf .
38 1948.
39 https://agoa.info/downloads/reports/15841.html.
40 Ibid.
41 https://core.ac.uk/download/pdf/189619104.pdf .
42 African Union convention on Cyber Security and Personal Data Protection (27 July 2014).
43 Article 14.
44 Section 48 & 49, Data Protection Act 2019.
45 https://rm.coe.int/3148-afc2018-ws4-auc/16808e6875.
46 https://www.internetsociety.org/wp-content/uploads/2018/05/AUCPrivacyGuidelines_2018508_EN.pdf .

47 https://www.itu.int/en/ITU-D/Capacity-Building/Documents/IG_workshop_August2018/Presentations/Session%207_Verengai%20Mabika.pdf .
48 http://repository.eac.int:8080/bitstream/handle/11671/1815/EAC%20Framework%20for%20Cyberlaws.pdf?seq. p.18.
49 Regulation 38.
50 https://www.eac.int/common-market.
51 https://www.eac.int/documents/category/protocols.
52 Article 4(2).
53 Article 5(2).
54 Article 8.
55 Article 9(2).
56 https://www.knqa.go.ke/wp-content/uploads/2019/05/East-AQfrican-comon-market-protocol.pdf. p.6.
57 Aspen Network of Development Entrepreneurs: East Africa Legal Guide ANDE Legal Working Group Toolkit New Markets Lab Katrin Kuhlmann, 2015: https://cdn.ymaws.com/www.andeglobal.org/resource/dynamic/blogs/20160229_130731_31785.pdf.
58 https://www.tralac.org/resources/our-resources/6730-continental-free-trade-area-cfta.html.
59 Article 4.
60 Article 5(e).
61 Article 19.
62 Article 1(p).
63 Article 8.
64 Svetlana Yakovleva and Kristina Irion. *Pitching trade against privacy: reconciling EU governance of personal data flows with external trade : International Data Privacy Law, 2020, Vol. 10*, No. 3 p.202.
65 Ibid. p.40.
66 T. Sargsyan. *Data Localization and the role of Infrastructure for Surveillance, Privacy and Security*, American university USA, 2016.
67 Mona Farid Badran. *Economic impact of data localization in five selected African countries*, 2018.
68 Matthias Bauer, Hosuk Lee-Makiyama, Erik van der Marel, Bert Verschelde. *The Costs of data Localisation: Friendly Fire on Economic Recovery*, ECIPE Occasional Paper No. 3/2014 European Center for International Political Economy, 2014, http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf .
69 Mona Farid Badran. *Economic impact of data localization in five selected African countries*, 2018.
70 https://www.cigionline.org/static/documents/gcig_no30web_2.pdf .
71 https://www.businessdailyafrica.com/bd/corporate/technology/amazon-rollout-of-cloud-computing-unit-in-nairobi-set-to-spur-east-african-market-2270678.
72 https://telecoms.com/500992/us-government-to-consider-strict-data-localisation-laws/.
73 https://www.iif.com/Portals/0/Files/content/Innovation/12_22_2020_data_localization.pdf.
74 https://discover.cloudscene.com/market/data-centers-in-kenya/all.
75 https://cloudscene.com/market/data-centers-in-kenya/all.
76 Ibid. p.40.
77 https://ca.go.ke/wp-content/uploads/2018/09/Guidelines-on-the-use-of-Internet-of-Things-IoT-Devices.pdf .
78 http://www.connectingafrica.com/author.asp?section_id=761&doc_id=755875.
79 Article XX GATT.
80 https://cis-india.org/internet-governance/resources/the-localisation-gambit.pdf. p.44.
81 Article II GATS.
82 Section 48, Data Protection Act 2019.
83 https://www.weforum.org/agenda/2015/11/what-are-your-digital-rights-explainer/.
84 T. Sargsyan. Data *Localization and the role of Infrastructure for Surveillance, Privacy and Security*, American University, USA, 2016.
85 Ibid.
86 Ibid.

POLICY BRIEF 03

MANDELA INSTITUTE

ABOUT THE MANDELA INSTITUTE

The Mandela Institute is a centre in the School of Law of the University of the Witwatersrand. The Mandela Institute conducts research, develops policy and offers basic and advanced teaching in different areas of law. Further, the Institute conducts executive teaching, training and capacity-building through offering short-course certificate programmes, conferences, and public seminars in areas of law and policy which are domestic in operation but are impacted by global developments.

ABOUT THIS POLICY BRIEF

This Brief is part of a series of publications under the Mandela Institute's 2021 research project on The Economic Impact of Data Localisation in Africa. This project is funded by Facebook.

ABOUT THE AUTHOR

Malcolm Kijirah is an Admitted Attorney and Advocate of the High Court of Kenya and Australia and holds multiple degrees in Information Technology from Kenya and Australia.

Elaine Wangari Thuo is a research fellow of the Kenyan School of Internet Governance.

Mandela Institute, School of Law
School of Law Building
Braamfontein West Campus
University of the Witwatersrand
Johannesburg 2000
South Africa

www.wits.ac.za/mandelainstitute

Design and layout by COMPRESS.dsl | 400419 | www.compressdsl.com

MANDELA INSTITUTE, SCHOOL OF LAW, UNIVERSITY OF THE WITWATERSRAND

UNIVERSITY OF THE WITWATERSRAND, JOHANNESBURG