POLICY BRIEF 04

MANDELA INSTITUTE

THE (POTENTIAL) ECONOMIC IMPACT OF DATA LOCALISATION POLICIES ON NIGERIA'S REGIONAL TRADE OBLIGATIONS

Lukman Abdulrauf *and* Oyeniyi Abe

MANDELA INSTITUTE, SCHOOL OF LAW,
UNIVERSITY OF THE WITWATERSRAND

UNIVERSITY OF THE WITWATERSRAND, JOHANNESBURG

CONTENTS

1. INTRODUCTION

The protection of individuals, especially within the context of the processing of their personal information, has now become a global issue. The general norm across the world today is that countries are establishing various mechanisms (legal and non-legal) for protecting their citizens from the risks associated with the collection and usage of their personal information – especially with tremendous advances in technology. Among the mechanisms for protecting individuals is data nationalism or data localisation. This is a policy which requires that data or a copy thereof (both personal and non-personal) should only be stored and processed locally and should not be exported for processing.[1] The importance of this, for instance, is that all data generated within Nigeria must be confined to the boundaries of Nigeria, effectively restricting the flow of data.[2] There are many justifications for the localisation of data. Some of these justifications include the protection of privacy and ensuring effective 'economic control' over data that emanate from a country. Indeed, the United Nations Conference on Trade and Development (UNCTAD), in its Digital Economy Report (2019), observed that developing countries can only exercise 'effective economic "ownership" of and control over the data generated in their territories by restricting cross-border flows of important personal and community data'.[3]

While the localisation of data has significant economic and social benefits, it is also associated with several unintended (negative) consequences – especially from an economic perspective. This is especially true for developing countries like Nigeria. Nigeria is one of the few countries in the world that is moving towards greater data localisation with several policies skewed in that direction. This has severe implications for the economy and for its commitment under regional treaty law. For example, Nigeria, as a signatory to the African Continental Free Trade Area (AfCFTA) Agreement, committed to eliminating all forms of barrier to trade and to promoting movement of capital and natural persons. The requirement for localising data is no doubt one of the most aggressive non-tariff barriers to trade in both goods and services.

This paper specifically examines the implications of Nigeria's increasing move towards data localisation (especially in critical sectors such as finance and communications) on its regional obligations for the promotion of free trade in Africa. The key questions are: what is the effect of data localisation on Nigeria's regional trade obligation to foster economic integration; and how can the promotion of internal trade and protection of privacy be effectively reconciled from a policy perspective? The paper is organised into five sections. After the introduction, the intersection between data protection and data localisation within Nigeria's digital economy and the ensuing challenges are examined in the second section. Nigeria's commitment under regional treaty frameworks, particularly those imposing trade liberalisation obligations on the country, is analysed in the third section. In the fourth section, the effect of data localisation on Nigeria's regional treaty obligations is considered. The fifth section concludes the paper with a reflection on the broader issue of reconciling the potential conflicts between data localisation and trade liberalisation obligations.

2. DATA PROTECTION, DATA LOCALISATION AND NIGERIA'S DIGITAL ECONOMY

2.1 An overview of the digital economy in Nigeria

In a global space, the digital economy, also known as the 'internet economy', 'new economy' or 'web economy', is a force to be reckoned with because of the fast-paced expansion in this sphere.[4] In 2016, the global digital economy provided 15.5% of the world's overall gross domestic product (GDP), which was worth USD11.5 trillion. For many years, developing countries looked away from the digital mine while leaving developed nations such as the United States (US), the United Kingdom, Germany and Japan to soar high in developments through the deployment of digital technology.[5] Developing nations have realised that any development devoid of a technological basis is likely to fail.[6] Hence, the Nigerian government faces a need to re-orientate its oil-based economy and integrate digital technology to restructure its economy.[7] Therefore, recent trends have seen the introduction of economic policies and investments channelled towards developing information and communications technology (ICT) capacity and infrastructure necessary for facilitating a digital economy among local and international trade partners.[8] It is in line with this that the Nigerian government renamed the Federal Ministry of Communications the Federal Ministry of Communications and Digital Economy, in order to influence Nigeria's digital economic policy and strategy.[9]

Nigeria has also taken some steps in the past to influence its digital space. For instance, Nigeria's Economic Recovery and Growth Plan 2017–2020 (ERGP) has identified the need to make the Nigerian economy more competitive in the 21st century global economy by drawing up a digitally led strategy for this purpose.[10] In addition, in 2015, the Nigeria Communications Commission (NCC) proposed that the Nigerian economy be transformed

into a digital one; this was to be achieved by investing in digital infrastructure and particularly in broadband.[11] The National Bureau of Statistics (NBS), in its report, stated that Nigeria's digital economy, which is only still emerging, contributed over 4 trillion Naira to the country's GDP in 2019.[12] Furthermore, Nigeria plans to 'attain an up and running digital economy by 2023'.[13] While this may appear ambitious, the eight-pillar National Digital Economy Policy and Strategy was 'designed to harness the capacities of its agencies and properly blend them with the roles of the private sector, in building a flourishing digital economy for the benefit of Nigerians'.[14]

Nigeria is today described as the biggest economy in Africa and has one of the largest youth populations in the world.[15] However, it has not fully tapped into the benefits of a digital economy. The available ICT facilities and infrastructures in Nigeria are insufficient for the country to attain the level where it reaps the full benefit of the digital economy.

Regardless of the commitment of the Nigerian government to harness the underlying benefits of the digital economy, there are still several challenges. A low level of broadband penetration is one such challenge. Broadband provides major infrastructure for digital economy to thrive, yet its penetration level in Nigeria still stands at 37.8%.[16] Nigeria has been persistently ranked as one of the countries with the lowest broadband penetration in the world.[17] In assessing readiness for a digital economy, Nigeria continues to rank low (between 112 and 152 out of between 137 and 188 countries) with the following indices: technological readiness; ICT infrastructures; e-services; availability of local content; digital divide; human resources; and digital skills.[18] Yet another challenge to tapping into the resources of the digital economy is data localisation. We will now consider this issue in detail.

2.2 Data localisation and data protection in Nigeria

The unrestricted movement of data is a key enabler of the digital economy. However, the development of data protection and data localisation policies is becoming one major area of concern for international trade and investment.[19] This is especially true for e-commerce and internet-based services within countries, which heavily rely on cross-border data flow internationally.[20] Without a doubt, the unrestricted movement of data across borders comes at a cost. For one, it raises concerns associated with security, surveillance, law enforcement and, most significantly, the fact that unrestricted data flow exposes individuals to the risk of violation of their right to privacy and personal data. It is for this reason that countries establish data privacy regimes to curtail some of the risks associated with trans-border data flow.

As part of their efforts to regulate cross-border data flow, a growing number of emerging economies have, in addition, introduced data localisation measures. According to Chander and Le, data localisation measures are those measures that specifically encumber the transfer of data across national borders.[21] These measures cover far-reaching rules and regulations prohibiting the exportation of information to countries with lighter regulation, which merely requires the prior consent of a data subject before their personal information is transmitted. Lighter measures also include rules requiring copies of data to be stored domestically and rules imposing tax on data export.[22] Therefore, the approaches of countries to data localisation range from those with strict to those with lighter measures.

Nigeria is also recognised as one of the emerging world economies with a strict requirement for localisation of data restricting the flow of data across borders. There is no specific *sui generis* data privacy law, even though the right to privacy is guaranteed by the Constitution of the Federal Republic of Nigeria (1999).[23] However, the National Information Technology Development Agency (NITDA), in 2019, introduced the Nigeria Data Protection Regulation (NDPR), which guarantees data privacy and ensures that Nigerian companies are competitive in international trade.[24] The NDPR is so far the most significant data privacy instrument in Nigeria, which is to be enforced by NITDA. Apart from the NDPR, other more specific data localisation rules and regulations exist. We will now consider these regulations.

2.2.1 NITDA regulations and policies on data localisation

Apart from the NDPR with its potential data-localising effect, NITDA has also pushed for data localisation through various legal instruments. It recently published its privacy policy to guarantee the privacy rights of all persons whose personal information are stored in the database of the agency. The policy also addresses 'clear negative trade balance' in the information technology (IT) sector by setting a target of 50% local content threshold for goods and services in the IT sector. To further this objective, NITDA introduced several measures purportedly to encourage indigenous innovation. The first measure is the release of the *Guidelines for Nigerian Content Development in Information and Communications Technology (ICT) 2013*.[25] These Guidelines require all indigenous original equipment manufacturers to assemble all hardware in Nigeria and to maintain fully staffed facilities for that purpose.[26] It also requires all telecommunications and network service companies to host all subscriber and consumer data in Nigeria.[27] To ensure data sovereignty, the Guidelines made further provisions that require that all ministries, departments and agencies (MDAs) in Nigeria host websites locally and under a registered '.gov.ng' domain.[28] Similarly, all data

and information management companies must host all sovereign data in Nigeria[29] and MDAs must host all sovereign data on local servers within Nigeria.[30]

In 2019, NITDA introduced another initiative with a data-localisation effect with the release of the *National Cloud Computing Policy* issued pursuant to Section 6 (a–c) of the NITDA Act.[31] The policy aims to promote the adoption of cloud computing by the Nigerian government and small and medium-sized enterprises (SMEs). The policy regards 'government data' as 'data produced or commissioned by government or government-controlled entities'.[32] This invariably covers a large collection of data and databases. More specifically, while the policy encourages cross-border data flow, it requires that 'agencies must do so in line with the requirements of the *Nigerian Data Protection Regulation* and any other content regulation'.[33] Thus, federal public institutions are only to contract cloud service providers that will store data in a jurisdiction that provides a level of data protection that is deemed equivalent to that of Nigeria, based on guidance provided by NITDA.[34]

> Nigeria is also recognised as one of the emerging world economies with a strict requirement for localisation of data restricting the flow of data across borders.

The benefits of data sovereignty and of harnessing the importance of cloud storage give some level of protection to investors and state actors. However, the lack of clarity and the inability to domesticate infrastructure have prevented the local economy from leveraging home-grown IT infrastructure rather than using external cloud service providers.[35] For example, local investors and entrepreneurs understand the intricacies of the technology and the operational costs of deploying cloud strategy. Because of the externalisation of costs and operations, Nigerians pay extremely high costs for internet services since the cloud support mechanisms are hosted externally. Data localisation thus becomes helpful in allowing home-grown investors to operate in the country.

In 2020, NITDA issued the *Guidelines for the Management of Personal Data by Public Institutions in Nigeria*. The Guidelines restrict the processing of personal data by public entities in accordance with the stipulations of the NDPR, based on the understanding that 'governments at all levels are the biggest processors of personal data of Nigerians and in Nigeria'.[36] The implication of these Guidelines is to restrict the processing of data held by public institutions except when based on well-defined circumstances.

2.2.2 The Nigerian Communications Commission's measures

The Nigerian Communications Commission (NCC) also contributes to data localisation with the NCC registration of the *Telephone Subscribers Regulations 2011*,[37] which provides for the privacy and protection of personal data of telephone subscribers in Regulations 9 and 10. Specifically, this Regulation imposes obligations on the licensees to ensure that the personal information of subscribers is stored in confidence. This information is not to be released to third parties nor to be transferred outside of Nigeria without first obtaining the consent of the subscriber and of the NCC. All information stored in the central database is regarded as the property of the federal government of Nigeria.[38]

2.2.3 The Central Bank of Nigeria's measures

The Central Bank of Nigeria (CBN), in exercising its powers under Section 47(3) of the Central Bank of Nigeria Act, 2007, issued the *Guidelines on Point of Sale (POS) Card Acceptance Services (POS Guidelines)*, which regulates all domestic transactions performed with the payment card. Specifically, Regulation 4.4.8 provides that:

> *'All domestic transactions including but not limited to POS and ATM transactions in Nigeria must be switched using the services of a local switch and shall not under any circumstance be routed outside Nigeria for switching between Nigerian Issuers and Acquirers'.*[39]

The implication of the above is to ensure the protection of data assessed by POS and ATM handlers.

2.2.4 Other measures

Apart from the above, there are other measures with potential effects on the localisation of data. For example, the Nigerian government recently launched the *Nigerian Content Development and the Cyber Security Policy and Strategy (NCPS) 2021* in order to strengthen cybersecurity governance and coordination.[40] The policy document aims at protecting personal data while upholding Nigerian sovereignty.[41] According to the national security adviser, Babagana Muguno, the policy seeks to, among others, improve indigenous technology development and safeguard critical infrastructure.[42]

Of all the above measures, the most significant is the *Data Protection Bill, 2020* – currently before the Nigerian national assembly. This Bill is the proposed overarching data protection legislation, which will replace the NDPR. Section 43 restricts trans-border data flow to countries

with an adequate level of data protection. The exceptions to this provision where data can be transferred are where the data subject provides consent or when based on specific interests of the data subject or prevailing legitimate interest.[43] It is still unclear who determines the adequacy of the regime of a third country.

From the foregoing, it is apposite to state that even if a regulation/provision is not explicit on data localisation, the more complicated the procedure for data transfer, the more restrictive it is. Thus, despite some of the good motives of data localisation measures, this could have an implication on Nigeria's obligations – especially under international and regional trade law. Consequently, it is necessary to ask: are Nigeria's data localisation measures an impediment to trade facilitation, and therefore counterproductive? Is Nigeria's privacy concern legitimate? These and some other concerns will be addressed in the next section.

3. DATA LOCALISATION, INTERNATIONAL AND REGIONAL TRADE LAW AND NIGERIA'S OBLIGATIONS

The Nigerian economy is acknowledged to be the largest in Africa and the 26th largest in the world, and as such any policy that affects trade would not only affect the country, but may affect its relationship with Africa and the world at large.[44] The country has, over the years, tried to use trade, including international and regional trade, to stimulate its economic potential.[45] According to John Onyido et al.,[46] 'no single economy can thrive meaningfully or is sustainable over the long term without external trade'. Consequently, Nigeria's trade agreements must not only be sustainable, but must meet the demands of the future through easier access to e-commerce and trade benefits. It is in line with this that the nation has entered several trade agreements and has ratified certain international and regional trade treaties.

Since Nigeria joined the World Trade Organisation (WTO), it has entered several trade and bilateral agreements. These agreements are geared towards enhancing trade and investment opportunities between the parties.[47] For example, the African Growth and Opportunity Act (AGOA) expands the trade and investment relations between the US and sub-Saharan Africa, whereas the Economic Community of West African States (ECOWAS) Trade Liberalization Scheme is a trading instrument that offers unrestricted market access to the 15 member countries and promotes economic relations within the sub-region. Below is an analysis of some of these trade instruments, to which Nigeria is a party, and the specific nature of the obligations arising from them.

> The application of the principle of technological neutrality in Nigeria, whereby data localisation requirements prevent access to the online delivery of services, could be a breach of Nigeria's commitment under treaty frameworks.

3.1 The AfCFTA

Pursuant to the *Lagos Plan of Action, 1980*,[48] the African Union (AU) began the creation of the African Economic Community through a free trade area, customs union and a common market amongst the 55 African Member States.[49] To achieve greater cohesion and economic integration within the continent, the AfCFTA Agreement was created. The Agreement seeks to make intra-African trade easier and more competitive through the minimisation of tariff and non-tariff barriers and gradual elimination of 90% tariffs within five to fifteen years.[50]

Nigeria signed the AfCFTA Agreement in July 2019 and ratified the Agreement on 5 December 2020.[51] The Agreement is aimed at increasing intra-African trade by creating a liberalised market and by delivering a wide-ranging and constructive trade agreement among the Member States.[52] The main objectives of AfCFTA are to: create a single continental market for goods and services, with free movement of business persons and investments; expand intra-Africa trade across the regional economic communities and the continent in general and; enhance competitiveness and support economic transformation.[53] AfCFTA has eased the flow of services and information among member countries and its resultant effect is that there is an obligation on each Member State to ensure the free flow of data, including personal data of their citizens, to other member countries. This is especially necessary for digital trade and e-commerce. Invariably, this creates a sharp contrast between the objectives of AfCFTA and Nigeria's data localisation policies. Thus, the data protection frameworks in Nigeria need to be compatible with the international trade regime if it is to benefit from the global digital economy under the several bilateral and multilateral trade agreements to which the country is a party.[54]

AfCFTA provides a significant avenue for Nigeria to enhance its trade relations with other African states.

However, implementation remains a challenge. On the one hand, lowering tariffs could help diffuse trade challenges, while on the other, restructuring non-tariff and trade facilitation measures may cause significant policy reforms at national level. To remain competitive and to confront Africa's economic fragmentation, trade barriers must be eliminated.[55] However, significant barriers – such as non-tariff barriers in services, fragmented rules designed to promote investment and data localisation policies – impede trade facilitation.[56] Protectionist policies such as data localisation can be maintained in such sectors that do not contribute significantly to the economy. Deepening regional integration calls for heightened scrutiny on cross-border trade, which goes undetected.[57] The eradication or non-deference to data localisation will foster economic transactions and reduce the 'prices of imported goods for consumers and producers using intermediate inputs'.[58] Since not all countries have data localisation policies within the continent, Nigeria's data localisation policies will no doubt create an onerous administrative process, therefore stifling trade. This means that data protection as a policy objective must be adapted in trade rules governing data transfers.[59] Application of different rules and domestic regulations may frustrate the aims of AfCFTA, thereby leading to compliance and operational costs.[60]

Within the rubric of trade facilitation guaranteed under WTO rules, AfCFTA becomes instructive. However, the invention and implementation of AfCFTA could become a mirage where protectionist measures conflate with free trade obligations. In the next section, we will discuss Nigeria's trade obligations under various bilateral agreements and the multilateral trading system of the WTO. We consider the importance of a steady, malleable and harmonious data localisation measure that could facilitate trade. Otherwise, protectionist measures that hamper trade commitments could severely affect Nigeria's standing in the international trade community.

3.1.1 AfCFTA rules and data localisation

Nigeria's data localisation measures appear to align with local content requirements for employment generation and local investment. However, such policies could end up being counterproductive, as they may hinder international investment and trade facilitation. The phenomenon of regional trade agreements (RTA) encourages the cooperation between members of a trade arrangement. The WTO guarantees effortless, predictable and free flow of trade if there is no detrimental effect.[61] To ensure this, any form of obstacle must be removed. One such obstacle is data localisation by Member States. Granted that trade relations sometimes involve conflicting interests between investors, stake-holders and states, the actualisation of data localisation creates an extreme barrier to trade. Consequently, it appears as if AfCFTA does not regulate data localisation procedures. Rather, it provides some model of protection alongside actions, which constrains the 'cross-border transfer and storage of data',[62] particularly where such restrictions are aimed at international investors. Furthermore, AfCFTA does not seem to address the challenges imposed by such requirements that attempt to disregard national treatment and market access commitments for foreign investors. At the WTO level, there has been no dispute or challenge to data localisation measures. Hence, the extent to which Nigeria's data localisation requirements are allowed under WTO rules or whether they impede trade remains unclear.

Notably, the *General Agreement on Trade in Services* (GATS), 1995, allows Member States to 'regulate supply of services in pursuit of their own policy objectives'.[63] Services are not defined under the Agreement. However, Article 1.2 (a) defines 'trade in services' to include the supply of services from one country to another. Nigeria's commitment to GATS does not limit the provision of any services, except to show that all foreign commercial activities must be domesticated in Nigeria.[64] The application of the principle of technological neutrality in Nigeria, whereby data localisation requirements prevent access to the online delivery of services, could be a breach of Nigeria's commitment under treaty frameworks. As a result, where not sensitively applied, data localisation measures could breach Nigeria's market access and national treatment commitments under AfCFTA.Nigeria is yet to make a full commitment under AfCFTA. It is therefore difficult to conclude whether it can impose a market access barrier impeding foreign investors from operating in the domestic market. If Nigeria has made full commitments under AfCFTA, it cannot claim or require foreign investors to be domesticated before they can operate locally,[65] or restrict cross-border data transfers, especially through electronic means. For example, Nigeria could require international telecommunications traffic to be routed through a domestic carrier, instead of the preferred international carrier. This act could be in violation of Nigeria's commitment under regional and international treaties as it attempts to impose a zero quota on the cross-border supply of services. Besides, Article XVII of GATS prohibits any form of discrimination against foreign suppliers in sectors that Member States have committed to – including the telecommunication and financial sectors of Nigeria.

Data localisation measures that prevent the actualisation of the most favoured nation clause under WTO rules deserve some level of heightened scrutiny, especially regarding the 'effect and trade impact of the measure'.[66] A broadly couched data localisation protectionism measure will most certainly violate trade obligations and commitments under treaty regimes.[67] The exceptions to these trade rules allow Member States to deviate from market access and national treatment commitments.[68] These exceptions are anchored on public morals and

protecting the right to privacy may allow Nigeria to craft policies that could limit cross-border data transfers in the interests of policy measures. Hence, data protection laws that prevent data harvesting or the storage of data outside Nigeria to protect individual privacy, could fall under GATS exceptions. Consequently, Nigeria's commitments under its trade treaties could be jeopardised where data localisation measures limit the exercise of those commitments. However, this is inconclusive as there are no final decisions from the Appellate Body ruling with finality on the conflict between data localisation and commitments to free trade under bilateral agreements. Unfortunately, the absence of judicial examination 'considering data localisation measures means significant legal uncertainty remains about how such measures would be treated under the GATS'.[69]

3.1.2 AfCFTA regulations on cross-border data flow

Articles 6 and 15 (c) (ii) of AfCFTA's *Protocol on Trade in Services* regulate the ability of Member States to transfer and store data across national borders. While Article 6 prevents Nigeria from disclosing confidential information and data where such disclosure will impede law enforcement or be contrary to the public interest – 'prejudice legitimate commercial interests' of businesses[70] – the general exemption from the AfCFTA data provisions under Article 15 (c) (ii) allows Nigeria to adopt protectionist measures, such as data localisation, where such measures guarantee 'the protection of the privacy of individuals in relation to the processing and dissemination of personal data and protecting confidentiality of individual records and accounts'.[71]

> While AfCFTA does not have a protocol on cross-border data transfer, we believe that data localisation without adequate rationale disrupts the true intention of AfCFTA.

In effect, Article 6 facilitates cross-border data flow by permitting businesses to transfer data among Member States. However, where the transfer of data concerns any of the identified factors, such factors will be prohibited. For example, if a Nigerian telecommunications service supplier seeks to transfer data relating to its operations in South Africa to the suppliers' headquarters in Lagos, it may do so unless such transfer will obstruct law enforcement, will be contrary to public interests, and will prejudice legitimate commercial interests of other businesses. Furthermore, data localisation guaranteed under Article 15 (c) will only be justified where the reasons for such restrictions are not enforced in a way that will constitute 'arbitrary and unjustifiable discrimination' between Member States.[72]

A combined effect of these rules does not prevent State Parties from adopting trade restrictions in pursuit of legitimate commercial interest, provided such interests are not 'arbitrary and unjustifiable'. The horizontal effect of these provisions enables State Parties to craft a broad scope of policy objectives to protect their citizens. The question is how legitimate data localisation measures are in Nigeria to warrant consideration of policy objective determination. AfCFTA provides no guidance, and it is expected that any reason or policy goals on security, health or education would suffice.

Article 15 (c) (ii) of AfCFTA retroflexes the requirement under Article XIV (c) (ii) of GATS which provides that measures should not be applied arbitrarily. In effect, the AfCFTA data rules appear to be more expansive than the GATS approach as it includes data localisation measures that do not constitute 'breach of national treatment or market access' obligations of the WTO.[73] Thus, under the AfCFTA rules, Nigeria could require local and international investors to store data on servers within either Nigeria or a State Party's jurisdiction before commencing business. Such an action will not violate national treatment or market access as those acts are non-discriminatory.

The implication of these provisions is that multilateral and trade obligations protect data localisation measures where data is stored within the borders of Nigeria, despite the restriction of transferring data across borders. Both articles read jointly preserve the sovereignty of Member States to enact laws that restrict the flow of data subject to some exemptions. It is not yet clear how these provisions will be interpreted practically or before a dispute settlement body, given the new and innovative Agreement. However, for proper context, these articles must be read with the general objectives under Article 3 of the Protocol, which enhances the intentions of AfCFTA. The AfCFTA Agreement broadly seeks to achieve 'an integrated, prosperous and peaceful Africa' by creating a single and liberalised market for goods and services.[74] While AfCFTA does not have a protocol on cross-border data transfer, we believe that data localisation without adequate rationale disrupts the true intention of AfCFTA, despite the exception the Agreement grants in order to be involved in trade activities.

The AfCFTA provisions allow parties to preserve measures that appear to be inconsistent with the AU data protection regime. For instance, Article 14 (6) (a) of the *African Union Convention on Cyber Security and Personal Data Protection* (discussed below) prohibits data transfer to Non-member States except if 'the state ensures an adequate level of protection of the privacy, freedom, and fundamental rights of persons whose data are being or

are likely to be processed'.[75] While we concede that inadequate data protection can negatively affect market access and productivity, we are of the view that exceedingly rigid protection can constrain business activities with attendant unfavourable economic effects.

While AfCFTA contains some provisions on data protection and the conduct of trade, the remaining challenge is the dispute between provisions of regional instruments that impedes multilateralism guaranteed under WTO principles, which could have the capability of global trade distortion.

3.2 African Union Convention on Cyber Security and Personal Data Protection (The Malabo Convention)

The Malabo Convention is another instrument that creates trade obligations for Nigeria. Indeed, issues of cybercrime and cybersecurity have become worrisome in Africa. Specifically, cybercrime and cybersecurity could also be a trade barrier because it creates a lack of trust in an e-commerce platform. This fact is recognised even in the Convention's preamble where it is stated that 'the major obstacles to the development of electronic commerce in Africa are linked to security issues'.[76] *The Malabo Convention* therefore encourages AU Member States to recognise the need to protect personal data and to encourage the free flow of information to develop a credible digital space in Africa. Since the adoption of the Convention, only 30 out of 55 African nations have passed or drafted privacy laws and only 13 of them have data protection authorities.[77] This convention is brought about by the increase in international trade, international relations and cybercrime, which are all direct results of advancement in ICT.

Article 11 of this Convention encourages Member States to establish independent bodies to protect personal data, whereas Article 12 encourages Member States to establish limits on the processing and storage of data, with exception to public interest. The Convention significantly grants Member States the right to discontinue the processing of data, block some aspects of collected data and either temporarily or permanently prohibit data processing in emergency situations that affect fundamental rights and freedom.[78] A good example would be the collection of an individual's data for a lawful purpose and using such data for an unlawful purpose.

The Convention acknowledges the need to obey national constitutions and international law. In the Convention preamble, it also states that the establishment of a regulatory framework on cybersecurity and personal data protection should consider the need to respect the rights of citizens, which is guaranteed under the fundamental texts of domestic law and protected by international human rights conventions and treaties, particularly the *African Charter on Human and Peoples' Rights*. Importantly, the Convention urges Member States to establish legal and institutional frameworks for data protection and cybersecurity, which they could achieve by either establishing new institutions or use existing ones.

The Convention also outlines the principles that ought to be adhered to in processing personal data, such as consent and legitimacy; lawfulness and fairness; purpose, relevance, and storage of processed personal data; accuracy; transparency, confidentiality and security of personal data. It further enjoins state parties to prohibit any data collection and processing without consent that reveals racial, ethnic and regional origin, parental affiliation, political opinions, religious or philosophical beliefs, trade union membership, sex life and genetic information or data on the state of health of the data subject, except under certain exceptional circumstances.[79]

There are expectations that trade commitments must be adhered to. Furthermore, the creation of big data and data sharing frameworks without supervisory mechanisms could lead to state surveillance and violation of citizens' right to privacy, which contradicts the intent of data localisation measures.

3.3 ECOWAS Protocol on Free Movement of Persons, Goods and Services

ECOWAS is a regional group consisting of 15 members. Founded on 28 May 1975 through the Lagos Treaty, it was designed to encourage economic integration across the region.[80] Considered one of the pillars of the African Economic Community,[81] ECOWAS was also designed as a single large trading bloc 'through an economic and trading union'.[82] The Revised Treaty establishes a common market through trade liberalisation.

The fundamental objective of the organisation is to facilitate cooperation and development in economic activity, and various sectors of the economy, to contribute to the progress and development of the African continent.[83] It is against this backdrop that the *ECOWAS Protocol Relating to Free Movement of Persons, Residence and Establishment* was drafted on 29 May 1979 to facilitate the achievement of the set objectives of the regional organisation.[84] Consequently, the first phase of the protocol – the protocol on free movement of persons, goods and services was ratified in 1980 and national committees were set up in Member States to monitor and ensure the implementation of the protocol.[85] Understandably, data localisation measures will be in direct contrast with the right of citizens of ECOWAS Member States to establish businesses.

The *ECOWAS Protocol on the Free Movement of People and Goods* ensures free mobility of the community citizens. It allows citizens of Member States the right to enter and reside in the territory of another Member State, provided they possess a valid travel document and an international health certificate. However, it also allows Member States the right to refuse admission to any community – citizens who were inadmissible under the Member State's own domestic law.[86] While seeking to create a regional market for citizens of Member States, the goals speed up the socio-economic development of the region.

The Protocol does not define what constitutes goods or services, neither does it provide for cross-border data transfer. The only prohibition relates to persons who are inadmissible under the Member State's own domestic law. In facilitating economic activity within the sub-region, it appears as if this Protocol overrides any data protectionist measures of Member States to the extent that those measures prohibit the right to establish or restrict the free movement of services that encompass data.

3.4 ECOWAS Supplementary Act on Data Protection (2010)

ECOWAS is mindful of the need to promote regional trade among Member States and has recognised the fact that issues of data protection could be an obstacle to this goal. It is in light of this that the ECOWAS Supplementary Act was adopted. The Supplementary Act directly applies in Member States, and creates an obligation on members to 'establish a legal framework of protection for privacy of data relating to the collection, processing, transmission, storage, and use of personal data without prejudice to the general interest of the State'.[87] There is very little activity surrounding the implementation or actualisation of the Act. However, it remains a formidable instrument that balances the data privacy of citizens of Member States with the trade liberalisation objectives of the community.

3.5 West Africa–European Union Economic Partnership Agreement

The main aim of the *West Africa–European Union Economic Partnership Agreement (EPA)* is the establishment of a free trade area between Europe and West Africa in accordance with Article XXIV of the *General Agreement on Tariffs and Trade (GATT)*, through the gradual removal of trade restrictions between the two trade partners. The EPA is intended to foster the smooth and gradual integration of African, Caribbean and Pacific (ACP) states into the world economy, with due regard for their political choices and development priorities, thereby promoting their sustainable development and contribution to poverty eradication. EPA negotiations were officially launched at an all-ACP level on 27 September 2002.[88]

EPAs are legally binding bilateral contracts between the European Union (EU) and individual African countries. EPAs represent a fundamental shift in the trading relationships between the two parties, from a non-reciprocal preferential trading regime under which 'ACP' countries could export almost freely to the EU while maintaining their own restrictions on EU imports, to one requiring reciprocity in liberalisation, albeit with a certain degree of asymmetry in commitments, in line with rules of the WTO.[89] This, however, is as much a pyrrhic victory since prematurely opening markets translates into African agricultural and non-agricultural production finding it very difficult to compete with the most likely cheaper, perhaps better quality and even larger supply of goods and services from European countries.[90]

The EPA includes several safeguards that can be implemented if liberalised products are increasing too rapidly, thus endangering local markets. Data protection or localisation is not one of those safeguards. However, considering that the EPA is between the EU and West Africa as a bloc, no Member State will be allowed to evade its obligations under the Agreement as a result of domestic policies that do not relate to agricultural products. The EPA strongly advances West Africa's integration into the global trading system while supporting investment and economic development of the region.[91]

4. THE EFFECT OF NIGERIA'S DATA LOCALISATION POLICIES ON ITS TRADE LIBERALISATION OBLIGATIONS

The countless opportunities that digital technology offers[92] can be leveraged by developing countries, like Nigeria, to diversify their economy. These opportunities can be effectively harnessed with the unrestricted flow of both personal and non-personal data. The trade agreements to which Nigeria is a party to, create one overarching obligation – to ensure cross-border trade with no form of hindrance, especially at the regional level, while also protecting privacy (and other sovereign values). The implication of this huge obligation is that laws and policies put in place by the country must align with her free trade obligations, including data localisation policies. While data localisation measures significantly affect trade, especially in the information society, it also has many policy justifications. Indeed, according to John

Selby, 'proponents of data localisation laws have typically raised some or all of the following four arguments as justification for their recommendations: data localisation provides better information security against foreign intelligence agencies; data localisation supports the local technology industry; data localisation protects the privacy and security of citizens' data; and data localisation supports local law enforcement'.[93] In essence, the overall effect of the NITDA, NCC and CBN regulations and policies, which promote the localisation of data, are mainly justified on the grounds of privacy and the support of the local information technology industry. These localisation policies also have the effect of protecting Nigeria's digital sovereignty. While these are sound justifications, the question remains: how to reconcile these with Nigeria's free trade commitments discussed above.

The efforts made at domestic level to develop Nigeria's digital economy must be matched with a sustained commitment to its regional obligation. As mentioned, no nation can effectively develop today without paying close attention to the goldmine lying underneath the digital space. Nigeria's increasing move toward greater localisation of data with its many policies therefore has an impact on its commitment under international and regional treaty law – especially in the following crucial ways.

Localisation of data can cause unnecessary regulation of citizens since the government can easily control and monitor the data of citizens.

First, data localisation is a key barrier to digital trade. Indeed, traditional services can now be transacted across borders through digital means.[94] However, data is the hallmark of any digital transaction and where there are restrictions to the availability of data, this would throw a spanner in the works of digital trade.[95] Consequently, Nigeria's obligation to guarantee free trade under relevant treaties could be affected by its strict data localisation measures. In this regard, the US National Association of Manufacturers puts it succinctly that:

> *'…such trade barriers… take forms of not only traditional trade and investment restrictions, but also forced localisation barriers that pressure companies to move manufacturing and operations overseas, intellectual property theft that undercuts manufacturing competitiveness, problematic import and export policies that distort global trade and discriminatory technical barriers to trade that block imports and create advantages for domestic producers'.*[96]

In addition, data localisation may cause 'protectionist barriers that increase the cost of doing business in a country or region'.[97] For instance, because of the threats data localisation portends to American businesses, the US government has built safeguards against data localisation.[98] Data localisation policies have a tendency to restrict market accessibility, and this is against the free trade obligation to allow unhindered access to the Nigerian markets, including e-markets. For a country like Nigeria, struggling to diversity its economy, data localisation significantly affects trade in both goods and services. Second, Nigeria's data localisation drive leads to an increase in operational cost for global multinational companies with a potential back-end effect on consumers. Most trade agreements entered by Nigeria guarantee free trade at the best possible prices and stabilise export prices and commodity supply.[99] However, it is an established fact that data localisation will require that data is saved within a particular country. This means there is a duty imposed on the government to ensure an effective system and this would lead to higher operational costs for the country. Thus, to fulfil its free cross-border trade obligations, Nigeria will be required to store data at two places, and this would shoot up operational costs resulting in extra financial burden on the government, which is then passed on to consumers.[100] The resulting challenge is whether the goods being sold to Member States under the same trade agreements with Nigeria go for the 'best prices', while keeping the best interest of consumers in mind.

Third, data localisation leads to unhindered access of the government to personal data of individuals which are held by businesses. This points to data localisation as a potential tool for political repression: strict data localisation laws can enable a breach of privacy and data protection, anti-discrimination and freedom of expression, and democratic values.[101] More broadly, some observed that 'data localisation requirements could actually increase privacy risks by requiring data to be stored in single centralised locations that are more vulnerable to intrusion'.[102] Localisation of data can cause unnecessary regulation of citizens since the government can easily control and monitor the data of citizens. Where data localisation policies are too restrictive, it will have negative impacts on investments as no one wants to put their resources where there are too many administrative hurdles to cross in obtaining relevant data necessary for trade. In addition, this would be against the free trade agreements intended to guarantee cross-border trade with no form of hindrance.

Consequently, the disadvantages of data localisation far outweigh its benefits. Very few local entrepreneurs reap the benefits of data localisation, while the damage of data localisation is felt across all forms of businesses who will be prevented from accessing global services that could enhance their productivity. For instance, some

companies threatened to withdraw services from Nigeria after the release of its data localisation regulation.[103]

With the increasing rise in information digitisation, high-speed internet connectivity and cross-border data transfer, businesses are growing increasingly agitated by the ability of states to limit the free flow of such data, as such actions have the potential to stifle innovation and prevent the flow of digitally enabled services across jurisdictions.

The associated benefits of the multilateral trade regime and digitalisation can be disrupted by protectionist policies that inflict burdensome and exorbitant trade rules on businesses. Indeed, Nigeria's reason for data localisation is anchored on the local economic development rationale. However, evidence shows that data localisation has increased costs for local businesses, stifled innovation and technological inventiveness, and has impeded access to the global market by local entrepreneurs.[104] The increase in costs of doing business has also created forum shopping for businesses whereby it is less costly for businesses to use cloud services located outside Nigeria than it is for companies to pay for hosting such services within Nigeria.

5. CONCLUSION AND POLICY RECOMMENDATIONS

There is now a global recognition of the significance of a strong digital economy for the development of any country. This is only recently being appreciated by emerging economies such as Nigeria. Digital trade is one aspect that countries such as Nigeria should take seriously. Nigeria's current effort to begin actual trading under AfCFTA means that it has positioned itself as a resilient economy that boasts of attracting intra-Africa export diversification. Data localisation is, without a doubt, a significant non-tariff barrier to international trade and development and this has a severe impact on the growth and development of the economy. It is apposite to state that the localisation of data has some good justifications. Indeed, even the UN has, in a recent report, advised developing countries to restrict data flow for a variety of reasons – including protection of its citizens, security, and economic reasons.[105] However, these justifications must be reconciled with Nigeria's commitment under international and regional treaty frameworks of liberalising trade. This is also a significant fact to be taken into consideration, given the role and status of Nigeria on the continent. A pragmatic approach, which balances the justification for data localisation and trade objectives, must therefore be adopted. This is necessary given the many studies that have positively established that 'data localisation measures are in fact likely to undermine security, privacy, economic development, and innovation where adopted'.[106]

There are a lot of options open to policy-makers in Nigeria to effectively balance the protection sought from data localisation and its commitment under international and regional trade treaties. We recommend that every transaction must be dealt with on a case-by-case basis rather than having an overarching policy on localisation. In this regard, Nigeria can make use of other legal tools such as contract clauses, which compels companies/businesses to provide high levels of privacy and data protection. Similarly, certification and audits are also options that could secure the digital space for Nigerian citizens without affecting international trade.

Overall, there is a need for a region-wide emphatic statement on localisation. The AU must therefore put in place instruments, which explicitly recognises data localisation as a barrier to international trade and investment.

ENDNOTES

1 See Benjamin Vitaris, 'What is Data Localization? Meaning and Laws Explained' *Data Privacy*, September 29, 2020, https://permission.io/blog/data-localisation/.
2 UNCTAD, 'Digital Economy Report 2019', UNCTAD/DER/2019 https://unctad.org/system/files/official-document/der2019_en.pdf
3 UNCTAD, 'Digital Economy'.
4 Jacek Unold, 'Basic Aspects of the Digital Economy', *Acta Universitatis Lodziensis* 167, (2003): 41.
5 HA Zubairu, et al., 'Assessing the E-readiness of Nigeria for Digital Economy' *American Journal of Computer Science and Information Technology* 8, no.2 (2020): 50.
6 Zubairu et al., 'Assessing the E-readiness', 50.
7 Ibid.
8 Ibid.
9 Federal Ministry of Communications and Digital Economy, 'National Digital Economy Policy and Strategy (2020-2030),' https://www.ncc.gov.ng/docman-main/industry-statistics/policies-reports/883-national-digital-economy-policy-and-strategy/file
10 The World Bank, 'Nigeria Digital Economy Diagnostic: A Plan for Building Nigeria's Inclusive Digital Future,' https://www.worldbank.org/en/country/nigeria/publication/nigeria-digital-economy-diagnostic-a-plan-for-building-nigerias-inclusive-digital-future.
11 The World Bank, 'Nigeria Digital Economy'.
12 Salisu Na'inna Dambatta, 'Opinion: Nurturing Nigeria's Digital Economy,' The Will, July 14, 2020, https://thewillnigeria.com/news/opinion-nurturing-nigerias-digital-economy/
13 Dambatta, Nurturing Nigeria's Digital Economy'.
14 Ibid.
15 The World Bank, 'Nigeria Digital Economy Diagnostic Report' (2019) https://openknowledge.worldbank.org/bitstream/handle/10986/32743/Nigeria-Digital-Economy-Diagnostic-Report.pdf?sequence=1&isAllowed=y.
16 Zubairu et al., 'Assessing the E-readiness', 50. See also 'Nigerian National Broadband Plan 2020-2025', https://www.ncc.gov.ng/documents/880-nigerian-national-broadband-plan-2020-2025/file.
17 Zubairu et al., 'Assessing the E-readiness', 50.
18 Ibid.
19 GSMA, 'The Impact of Data Localisation Requirements on the Growth of Mobile Money-Enabled Remittances', https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/03/GSMA_Understanding-the-impact-of-data-localisation.pdf
20 GSMA, 'The Impact of Data Localisation'.
21 Anupam Chander and Uyen P Le, 'Data Nationalism', *Emory Law Journa*l 64, no.3 (2015): 680.
22 Ibid.
23 Lukman Adebisi Abdulrauf, 'Personal Data Protection in Nigeria: Reflections on Opportunities, Options and Challenges to Legal Reforms', *Liverpool Law Review* 38, (2016): 105–44. Andrew Ubaka Iwobi, 'Stumbling Uncertainly into the Digital Age: Nigeria's Futile Attempts to Devise a Credible Data Protection Regime', *Transnational Law and Contemporary Problems* 26, no.1 (2017):14-61.
24 NITDA, Section 1.1 of the NDPR, 2019 https://ndpr.nitda.gov.ng/Content/Doc/NigeriaDataProtectionRegulation.pdf.
25 'Guidelines for Nigerian Content Development in Information and Communications Technology (ICT)' https://nlipw.com/wp-content/uploads/Guidelines-for-Nigerian-Content-Development-in-Information-and-Communications-Technology-ICT.pdf.
26 'Guidelines for Nigerian Content Development', Guideline 9.1.
27 'Guidelines for Nigerian Content Development', Guideline 11.1(4).
28 'Guidelines for Nigerian Content Development', Guideline 12.2(1).
29 'Guidelines for Nigerian Content Development', Guideline 13.1(2).
30 'Guidelines for Nigerian Content Development', Guideline 13.2 (3).
31 NITDA, 'Nigeria Cloud Computing Policy' https://nitda.gov.ng/wp-content/uploads/2020/11/NCCPolicy_New1.pdf
32 NITDA, 'Nigeria Cloud Computing Policy', 5.
33 NITDA, 'Nigeria Cloud Computing Policy', 19.
34 Ibid.
35 Emma Okonji, 'Experts Highlight Benefits of Data Localisation, Cloud Adoption in Nigeria', *This Day*, November, 7, 2019, https://www.proquest.com/docview/2312365797?accountid=11526.
36 NITDA, 'Guidelines for the Management of Personal Data by Public Institutions in Nigeria' (2020), https://www.uubo.org/media/1950/nitda-guidelines.pdf section1.2.
37 NCC, 'Registrations of Telephone Subscribers' Regulations 2011', https://www.ncc.gov.ng/docman-main/legal-regulatory/regulations/201-regulations-on-the-registration-of-telecoms-subscribers/file.

38 Ibid.
39 CBN, 'Guidelines on Point of Sale (POS) Card Acceptance Services', https://www.cbn.gov.ng/cashless/POS_GUIDELINES_August2011_FINAL_FINAL%20(2).pdf.
40 Ibid.
41 Emma Okonji and Nosa Alekhuogie, 'NIMC: National Cybersecurity Policy Will Address Security Lapses', *This Day*, February 25, 2021.
42 Nelson Okoh, '2021 National Cybersecurity Policy and Strategy: Enhancing Digital Safety and Economic Growth', *The Journal*, June 25, 2021, https://thejournalnigeria.com/cybersecurity-policy-strategy-digital-safety-economic-growth/.
43 Data Protection Bill, Section 43(3).
44 John Onyido, Ibidolapo Bolu and Oluwasolape Owoyemi, 'Nigeria: Developments in Investment and Intraregional Trade in Africa', https://www.mondaq.com/nigeria/international-trade-investment/727066/developments-in-investment-and-intraregional-trade-in-africa?login=true.
45 Ibid.
46 Ibid.
47 Folarin Alayande, 'Understanding Shifts in Nigeria's Trade Policy: From Realism to Protectionism', *Africa Development* 45, no. 1 (2020): 149.
48 See the Treaty Establishing the African Economic Community, Lagos Plan of Action for the Economic Development of Africa 1980–2000 4 (1980); Adopted on 3 June 1991; entered into force on 12 May 1994.
49 See the Preamble and Art. 3 of the 'Agreement establishing the African Continental Free Trade Area (AfCFTA)'.
50 African Union, Report to the Specialized Technical Committee on Trade, Industry and Minerals: Progress on the African Continental Free Trade Area (AfCFTA) for the Period from May 2016 to Dec. 2018, 2& 3 (AUC/DTI/AfCFTA/STC/Rep/D). See further Oyeniyi Abe and Sewagegnehu Taye, 'The 'Flexibility' Standard in the African Union and Its Ramification for the Implementation of the African Continental Free Trade Area (AfCFTA) Agreement', *Global Trade and Customs Journal* 16, no. 2 (2021): 80.
51 'Status of AfCFTA Ratification', https://www.tralac.org/resources/infographic/13795-status-of-afcfta-ratification.html.
52 See the Agreement Establishing the African Continental Free Trade Area https://au.int/sites/default/files/treaties/36437-treaty-consolidated_text_on_cfta_-_en.pdf.
53 Tralac, 'The African Continental Free Trade Area: A Tralac Guide', https://www.tralac.org/documents/resources/booklets/4062-afcfta-a-tralac-guide-7th-edition-august-2020/file.html.
54 Tralac, 'Data Protection Regulations and International Data Flows: Implications for Trade and Development', April, 19, 2016 https://www.tralac.org/news/article/9500-data-protection-regulations-and-international-data-flows-implications-for-trade-and-development.html.
55 Neha Mishra, 'Data Localisation Laws in a Digital World', *Public Sphere*, 2016 Issue, (2016):137.
56 Maryla Maliszewska et al., *The African Continental Free Trade Area: Economic and Distributional Effects* (Washington: The World Bank, 2020).
57 Ibid.
58 Ibid.
59 Susannah Hodson, 'Applying WTO and FTA Disciplines to Data Localisation Measures', *World Trade Review* 18, no.4 (2019): 581.
60 See further Maryla Maliszewska et al., *The African Continental Free Trade Area*, 41.
61 Oyeniyi Abe, 'Deepening Regional Integration and Organizing World Trade: The Limits of ECOWAS', *International Journal of Public Law and Policy* 4, no.1 (2014): 72.
62 Hodson, 'Applying WTO and FTA Disciplines', 583.
63 Article XIX of the General Agreement on Trade in Services (GATS) https://www.wto.org/english/docs_e/legal_e/26-gats_01_e.htm.
64 'Nigeria, Schedule of Commitment's', https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=Q:/SCHD/GATS-SC/SC65.pdf&Open=True.
65 See further Article XVI, paragraph 2 of GATS.
66 Hodson, 'Applying WTO and FTA Disciplines', 592.
67 See Article XIV (a) (c) (ii) of GATS.
68 Article XIV (a) (c) (ii) of GATS.
69 Hodson, 'Applying WTO and FTA Disciplines', 596.
70 See Article 6 of AfCFTA's Protocol on Trade in Services.
71 Article 15 (c) (ii) of AfCFTA's Protocol on Trade in Services.
72 Article 15 (c) (ii) of AfCFTA's Protocol on Trade in Services.
73 Hodson, 'Applying WTO and FTA Disciplines',605.
74 See Article 3 of AfCFTA Agreement. See also Article 3 (2) (e) of AfCFTA's Protocol on Trade in Services.
75 Close variant to this is in Article 36 of ECOWAS Supplementary Act A/SA.1.01.10 on Personal Data Protection Within ECOWAS https://www.statewatch.org/media/documents/news/2013/mar/ecowas-dp-act.pdf.
76 See the Preamble to the AU Convention.

77 Abdi Latif Dahir, 'Africa isn't Ready to Protect its Citizens Personal Data Even as EU Champions Digital Privacy,' *Quartz Africa*, May 7, 2018, https://qz.com/africa/1271756/africa-isnt-ready-to-protect-its-citizens-personal-data-even-as-eu-champions-digital-privacy/.

78 Kaitlin M Ball, 'Introductory Note to African Union Convention on Cyber Security and Personal Data Protection', *International Legal Materials* 56, (2017):164.

79 See generally Lukman Adebisi Abdulrauf and Charles Manga Fombad, 'The African Union's Data Protection Convention 2014: A Possible Cause for Celebration of Human Rights in Africa?,' *Journal of Media Law* 8, no. 1(2016): 67.

80 See Economic Community of West African States 'Basic Information', https://www.ecowas.int/about-ecowas/basic-information/

81 Article 1 of the Economic Community of West African States (ECOWAS) Revised Treaty, https://www.ecowas.int/wp-content/uploads/2015/01/Revised-treaty.pdf.

82 Abe, 'Deepening Regional Integration', 74.

83 ECOWAS Treaty, 1975; Article 2.

84 ECOWAS Protocol on Free Movement of Persons and the Right of Residence and Establishment A/P.1//5/79.

85 ECOWAS Protocol on Free Movement of Persons and the Right of Residence and Establishment A/P.1//5/79.

86 Abimbola Opanike and Ayodeji Anthony Aduloju 'ECOWAS Protocol on Free Movement and Trans-border Security in West Africa', *Journal of Civil and Legal Sciences* 4, no. 3 (2015):154.

87 Article 2.

88 ECOWAS, 'Economic Partnership Agreement', https://www.ecowas.int/doing-business-in-ecowas/epa/.

89 Kelechi C. Nnamdi and Kingsley C Iheakaram, 'Impact of Economic Partnership Agreements (EPA) on African Economy: A Legal Perspective', http://cega.berkeley.edu/assets/miscellaneous_files/6-ABCA-Nnamdi-Impact_of_EPA_on_AFR_economy.pdf.

90 Nnamdi and Iheakaram, 'Impact of Economic Partnership Agreements'.

91 European Commission, "West Africa" <https://ec.europa.eu/trade/policy/countries-and-regions/regions/west-africa/>

92 Particularly because data collection and storage is an integral part of digital technology and because data is now regarded as the new oil.

93 John Selby, 'Data Localisation Laws: Trade Barriers or Legitimate Responses to Cyber-security Risks, or both?, *International Journal of Law and Information Technology* 25, no. 3 (2017): 213.

94 J Ferencz and F Gonzales, 'Barriers to Trade in Digitally Enabled Services in the G20', OECD Trade Policy Papers, no. 232, https://www.oecd-ilibrary.org/trade/barriers-to-trade-in-digitally-enabled-services-in-the-g20_264c4c02-en.

95 Hoagland Isabelle, 'Business, Tech Groups Flag Data Localisation Policies as Barriers to U.S', *Inside US Trade* 36, no. 45 (2018) https://www.proquest.com/docview/2131157486/fulltext/76D7F648B1B04C96PQ/1?accountid=11526.

96 Ibid.

97 Jennifer Huddleston and Jacqueline Varas, 'Impact of Data Localisation Requirements on Commerce and Innovation', *Insight* June 16, 2020, https://www.americanactionforum.org/insight/impact-of-data-localisation-requirements-on-commerce-and-innovation/.

98 Theodore Claypoole, 'Data Localisation and the Limits of 'Everything from Everywhere' https://www.womblebonddickinson.com/us/insights/articles-and-briefings/data-localisation-and-limits-everything-everywhere.

99 For instance, the International Commodity Agreements (ICAs).

100 Diganth Raj Sehgal, 'Data Localization and Cross-border Data Transfers', https://blog.ipleaders.in/data-localization-cross-border-data-transfers/.

101 Erica Fraser, 'Data Localisation and the Balkanisation of the Internet', *SCRIPTed* 13, no.3 (2016): 360-73.

102 Export Council of Australia, 2018.

103 International Trade Administration, 'Nigeria-Country Commercial Guide' https://www.trade.gov/knowledge-product/nigeria-market-challenges.

104 See further Chander and Le, 'Data Nationalism', 721.

105 UNCTAD, 'Digital Economy Report 2019', UNCTAD/DER/2019 https://unctad.org/system/files/official-document/der2019_en.pdf.

106 Chander and Le, 'Data Nationalism', 681. See also Selby, Data Localization Laws', 213.

POLICY BRIEF 04

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

Lukman Abdulrauf holds a PhD from the University of Pretoria with expertise in data privacy. He is a Senior Lecturer at University of Ilorin. Oyeniyi Abe holds a PhD from the University of Cape Town with expertise in Business and Human Rights. He is a Senior Research Fellow at OGEES Institute, Afe Babalola University and at the Centre for Comparative Law in Africa, UCT.

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 | 400430 | www.compressdsl.com

MANDELA INSTITUTE, SCHOOL OF LAW, UNIVERSITY OF THE WITWATERSRAND

UNIVERSITY OF THE WITWATERSRAND, JOHANNESBURG